The constant increase in the number of threats to the security of critical infrastructure objects, which include socio-cyberphysical systems, leads to a decrease in the quality of security services and the level of security of infrastructure elements. The object of research is the process of building a complex system of protection in socio-cyberphysical systems. The imperfection of the mechanisms for ensuring the security of critical infrastructure objects, which include socio-cyberphysical systems, the technological complexity of identifying new security threats necessitates an urgent need for a radical revision of the current approaches to its provision. So, it becomes clear that the development of a new approach to ensuring the security of information resources in socio-cyberphysical systems is needed. The article proposes a new approach to the methodological foundations of building multi-contour information protection systems with internal and external circuits on each of the platforms of socio-cyberphysical systems. This approach is based on a universal classifier of threats, which takes into account not the technical aspect of threats, but also their integration with social engineering methods, their synergy of hybridity. The socio-political influence on the realization of threats is taken into account, and practical mechanisms for providing basic security services based on post-quantum algorithms are also proposed. To provide basic security services in the proposed multi-contour protection system, it is proposed to use post-quantum algorithms – McEliece crypto-code constructions, which provide Perr=10^{-9}–10^{-12}, safe time Tsec=10^{25}–10^{35} group operations. Within the framework of the proposed approach, the problem of increasing the level of information security has been formalized and further ways of solving it have been determined

Keywords: *socio-cyberphysical system, cyber security, information security, security of information, critical infrastructure facilities*

UDC 623.618.51
DOI: 10.15587/1729-4061.2024.298844

DEVELOPMENT OF THE SOCIOCYBERPHYSICAL SYSTEMS` MULTI-CONTOUR SECURITY METHODOLOGY

Stanislav Milevskyi
PhD, Associate Professor*
Olha Korol
Corresponding author
PhD, Associate Professor*
E-mail: korol.olha2016@gmail.com
Galyna Mykytyn
Doctor of Technical Sciences, Professor
Department of Information Security
Lviv Polytechnic National University
S. Bandery str., 12, Lviv, Ukraine, 79013
Iryna Lozova
Senior Lecturer
Department of Information Technology Security
National Aviation University
Liubomyra Huzara ave., 1, Kyiv, Ukraine, 03058
Svetlana Solnyshkova
PhD, Associate Professor
Department of Physics and Electronics**
Iryna Husarova
PhD, Associate Professor
Department of Applied Mathematics
Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166
Alla Hrebeniuk
PhD, Senior Researcher
Scientific Laboratory
National Academy of the Security Service of Ukraine
Maksymovycha str., 22, Kyiv, Ukraine, 03022
Andrii Vlasov
PhD, Senior Researcher***
Vladyslav Sukhoteplyi
Department of Radioelectronic Systems of Control Points of Air Forces**
Dmytro Balagura
PhD***
*Department of Cybersecurity
National Technical University "Kharkiv Polytechnic Institute"
Kyrpychva str., 2, Kharkiv, Ukraine, 61002
**Ivan Kozhedub Kharkiv National Air Force University
Sumska str., 77/79, Kharkiv, Ukraine, 61003
***Department of Information Technology Security
Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166

Received date 30.11.2023
Accepted date 13.02.2024
Published date 28.02.2024

How to Cite: *Milevskyi, S., Korol, O., Mykytyn, G., Lozova, I., Solnyshkova, S., Husarova, I., Hrebeniuk, A., Vlasov, A., Sukhoteplyi, V., Balagura, D. (2024). Development of the sociocyberphysical systems` multi-contour security methodology. Eastern-European Journal of Enterprise Technologies, 1 (9 (127)), 34–51. doi: https://doi.org/10.15587/1729-4061.2024.298844*

1. Introduction

An important role in ensuring the national security of the state and especially its economic component is assigned to processes related to the protection of state market fundamentals that determine the economic component of competition. Revolutionary changes in infocommunication and computer networks made it possible to form a unification into a single information-cybernetic space, systems based on smart technologies, and led to the formation of socio-cyberphysical systems (SCPS) and the revision of critical infrastructure facilities (CIF). As a result, the range of threats to the national security of the state as a whole has increased significantly. The key and most potentially dangerous of

them is the threat of disruption or taking under remote control of control processes in socio-cyberphysical systems. At the same time, SCPS is understood as the evolutionary integration of smart technologies with social networks and messengers. A block diagram of socio-cyberphysical systems is presented in Fig. 1 [1–3].

The consequences of the absence or imperfection of security mechanisms in the SCPS (CIF) can be colossal and irreversible, resulting in the collapse of the financial and political system of the state. The solution to the entire range of issues related to ensuring cybersecurity (CS), information security (IS) and security of information (SI) in SCPS (CIF) must be resolved in a comprehensive manner and inextricably from one another. Simply combining forces and means in each individual case to ensure the security of socio-cyberphysical systems (critical infrastructure objects) is inappropriate, both from a practical and scientific point of view. The lack of other alternative approaches prompts an urgent need to solve the current problem – increasing the security of information in socio-cyberphysical systems based on new approaches unknown to date. This approach requires reformatting the mechanisms for constructing security systems for infrastructure elements and requires taking into account the construction of multi-contour information security systems based on post-quantum algorithms [4–6].

It is known that computer systems and telecommunications ensure the reliable functioning of a huge number of information systems for various purposes. Most of these systems contain restricted access information that is confidential. Thus, solving the problem of automating data processing processes entailed the generation of a new problem – the problem of information security [7–9]. Since their inception, social networks and instant messengers have always attracted criminal interest. And this interest was associated not only with the storage of personal data, but also with the possibility of using it as a cyber weapon in the implementation of both political and socio-economic influence projects. At the same time, regardless of the means, mechanisms and technologies used to ensure information security, another pressing problem is ensuring the information security of the individual, society and the state [10–12]. Data security during storage requires the use of encryption tools that can operate either at the level of data storage or at the level of individual system components, for example, database tables. Security in socio-cyberphysical systems must be ensured using post-quantum algorithms, as well as lightweight encryption algorithms that can be used in low-energy elements of socio-cyberphysical systems. Thus, the problem of cybersecurity is also an integral third component in solving the problem of ensuring the security of banking information [13–16]. Thus, an urgent problem is the need for a new approach to building information security systems that will ensure the required level of SCPS security (CIF) in the post-quantum period.

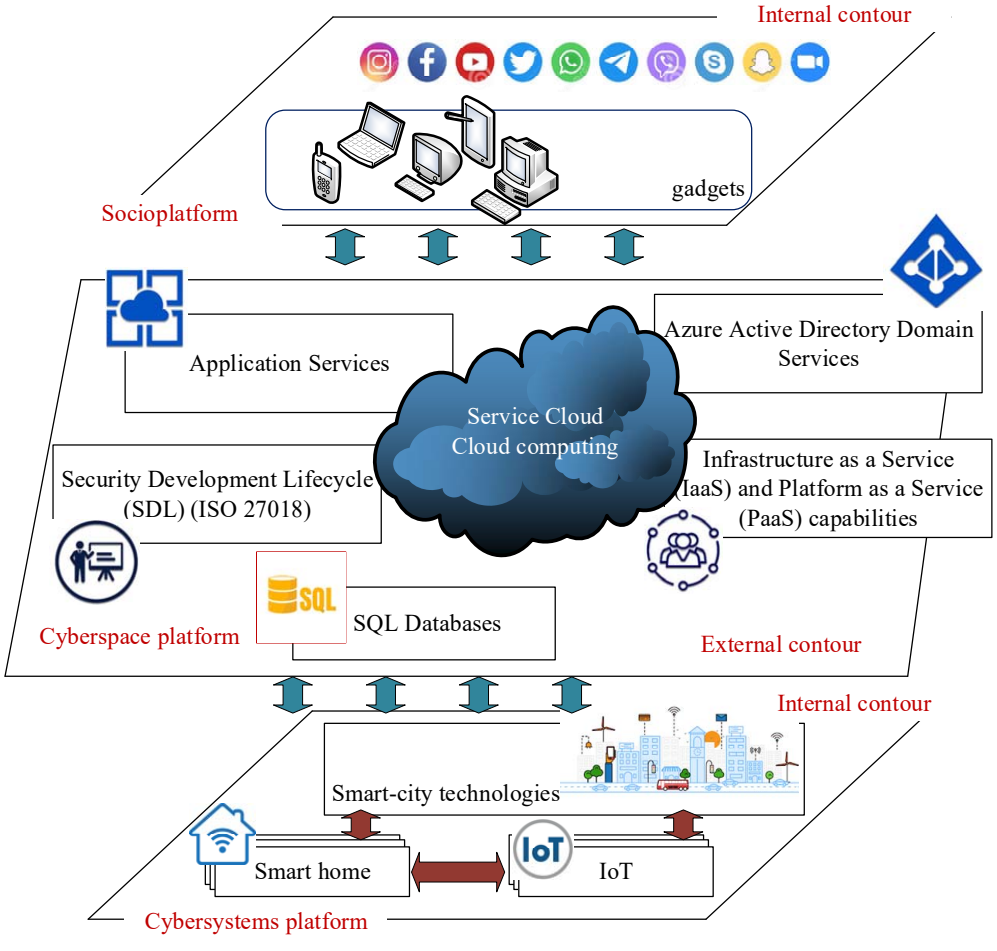

Fig. 1. Structural-logical diagram of socio-cyberphysical systems

2. Analysis of literature data and problem statement

In [1], crypto-code constructions (CCC) based on elliptic codes and their modifications are proposed, however, in smart technologies with limitations in computational and capacitive parameters, their use is not always possible. In addition, LDPC codes are already used in wireless channels, which simplifies the practical implementation (implementation) of CCC.

The analysis of the work [2] showed that international regulators consider the issue of building information security systems as separate aspects for each of the security components. However, this approach does not allow not only to form the methodological basis for constructing security systems, but also to take into account the evolutionary development of targeted attacks and complex threats.

The work [3] proposes models for constructing multi-contour systems; however, the integration of targeted threats with social engineering methods is not taken into account, which does not allow for an objective assessment of the current state of socio-cyberphysical systems` security.

The work [17] considers the issues of a new approach to building protection systems based on international regulators and taking into account the conduct of hybrid wars. However, the authors do not consider the possibility of building multi-contour systems, do not take into account the platform nature of modern critical infrastructure objects and their evolutionary development into socio-cyberphysical systems.

In [18], the authors classify, analyze threats and opportunities to increase the security level of pseudorandom number generators, and also define standards and testing methods to improve the reliability, security and eliminate vulnerabilities of such generators. However, their use in smart technologies is limited by computing and energy capabilities, which requires either the use of less crypto-resistant generators or requires the development of new approaches to ensure their strength.

In [19], the author proposes the "Security as a Code" methodology – security in cloud environments, which consists of integrating security controls, policies and best practices directly into the processes of software development and deployment. The integration process involves the transformation of security requirements and configurations into software code, which in turn is considered as an integral part of the complete software development life cycle. However, this approach does not take into account the requirements for the construction of multi-contour systems, integration and hybridity of targeted (mixed) threats.

An analysis of work [20] showed that to build security systems, a careful selection of not only metrics, but also classification of threats is required. However, the proposed risk assessment methodology does not take into account the complexity and synergy of target threats.

An analysis of international practices for protecting critical infrastructure facilities in [21] showed the need to integrate protection mechanisms for all security components: cybersecurity (CS), information security (IS) and security of information (SI). However, issues of increasing the level of resistance of the security mechanisms themselves have not been considered, and issues of changing to post-quantum algorithms have not been considered.

The study [22] examined the practical aspects of the methodology for assessing regional infrastructure (critical infrastructure facilities). However, the issues of ensuring the security of such objects have not been considered, taking into account the scaling and integration of technologies – the use of various standards and technologies of data circulation channels, Internet of things and smart technologies.

In [23], the methodology of "Improving the security of European critical infrastructure facilities" is considered, the basis of which is the concept of the risk of "loss of critical infrastructure" as an anthropogenic risk. The main disadvantages in assessing risks in [23] are the lack of integration when assessing the socio-political situation. In addition, the authors do not consider the influence of social aspects, social networks and messengers on cyber-physical systems and do not ensure the formation of multi-contour information protection systems of socio-cyberphysical systems.

The work [24] describes a methodology and its implementation for the assessment of critical infrastructures on a European scale. The methodology considers asset-level impacts, estimates the propagation of network-level failure due to interdependencies, and estimates the economic impact of critical infrastructure failures at the national level. However, the methodology does not take into account aspects of building multi-circuit information protection systems for each of the platforms of socio-cyberphysical systems (critical infrastructure facilities).

An analysis of work [25] showed the need to take into account the socio-political situation in society to prevent threats at critical infrastructure facilities. However, this does not take into account the aspects of how and in what way the assessment needs to be carried out, and what mechanisms need to be used in the context of the rapid growth of smart technologies and targeted attacks.

In [26], aspects of building a national defense system are considered – ways to protect society from terrorist attacks, natural disasters and other threats and dangers. However, the authors do not take into account the platform nature of socio-cyberphysical systems, as well as the need to consider security issues at each of the contours (internal and external) of the information security system.

Thus, the analysis showed that the evolutionary development of technologies and the capabilities of computing systems, on the one hand, make it possible to minimize energy and computational costs and form socio-cyberphysical systems. On the other hand, they do not take into account the capabilities of cyberterrorists, cyber groups, their computing and financial capabilities. Integrating threats with social engineering methods makes it possible to create mixed threats with characteristics of synergy and hybridity, which increases the risk of their implementation. The pursuit of super speeds in mobile technologies and their use (as the basis of communication) in smart technologies "ensures" the implementation of targeted attacks with a probability of more than 95 %. The absence of regulators at the international level of the need to integrate security mechanisms (to obtain emergent security properties) does not allow the formation of comprehensive information security systems. In addition, when building multi-contour information security systems, it is necessary to take into account the socio-political-economic situation in society and the state as a whole. To build multi-contour information protection systems for critical infrastructure facilities (socio-cyberphysical systems), it is necessary to use fundamentally new information protection mechanisms based on post-quantum algorithms.

3. Purpose and objectives of the research

The purpose of this research is to develop a methodology for constructing multi-contour information security systems in socio-cyberphysical systems based on post-quantum algorithms and taking into account the multi-contour nature of the security system. This will allow to obtain a fundamentally new approach to the formation of not only the classification of cyber threats, but also to build multi-contour protection systems. At the same time, for each platform, threats to basic security services in each contour (internal and external) are considered, which will allow to obtain an objective assessment of the critical points of the infrastructure, an objective assessment of the current state of protection. This approach also creates new opportunities for the timely development of preventive protective measures.

To achieve the purpose of the work it is necessary to solve the following tasks:

– to develop security mechanisms based on post-quantum algorithms;

– to construct a block diagram of the methodology for constructing a multi-contour information security system in socio-cyberphysical systems.

4. Materials and research methods

The object of the study is the process of building a comprehensive information security system in socio-cyberphysical systems. The current situation is not least due to the imperfection of the mechanisms used today to ensure the security of elements of critical infrastructure facilities, which include socio-cyberphysical systems.

The research hypothesis was as follows. To provide security services in socio-cyberphysical systems (critical infrastructure objects), it is proposed to use post-quantum crypto-algorithms based on McEliece's crypto-code constructions [1–3, 27–33]. The use of various noise-resistant codes makes it possible to ensure the required characteristics of both standard channels of information and communication systems and networks, and smart technology channels (wireless channels), as well as the transmission of various contexts (files, video, sound, etc.) [34–39]. In addition, the research carried out [1–3, 27–39] makes it possible to use various algebrogeometric codes, LDPC codes with defective codes, which makes it possible to build hybrid crypto-code constructions and provide the required efficiency and strength of confidential cryptography. The initial data for constructing such structures is the required parameters of durability and efficiency of transmitted information.

To build multi-contour security systems, let's use a threat classifier that takes into account hybridity, synergy and integration of mixed threats with social engineering methods. The practical implementation of the classifier is given in the resource [39], the main stages of the formation of a multi-contour information security system for socio-cyberphysical systems [6, 40, 41].

To assess the influence of the socio-political situation in a society (region), it is proposed to use the approach presented in [42], which makes it possible to ensure the use of the results obtained for models based on Lotka-Volterra [43]. Thus, the proposed mechanisms make it possible to formulate the methodological basis for constructing multi-circuit information security systems in socio-cyberphysical systems.

5. Development of a methodology for constructing multi-contour security systems

5. 1. Development of security mechanisms based on post-quantum algorithms

To provide security services in socio-cyberphysical systems, it is proposed to use post-quantum algorithms – crypto-code constructions based on LDPC codes with damage [33, 44–52]. However, the presented practical protocols for decrypting LDPC codes are based on soft decoding, which significantly affects decoding speed and reliability. The LDPC code check matrix is used for construction. For use in McEliece crypto-code constructions, a generating matrix is required, which can be obtained based on the orthogonality property of the check and generating matrices. To implement hybrid McEliece crypto-code constructions on LDPC codes with damage, let's use approaches which structural diagram of data transmission is shown in Fig. 2 [1, 28, 30, 33].

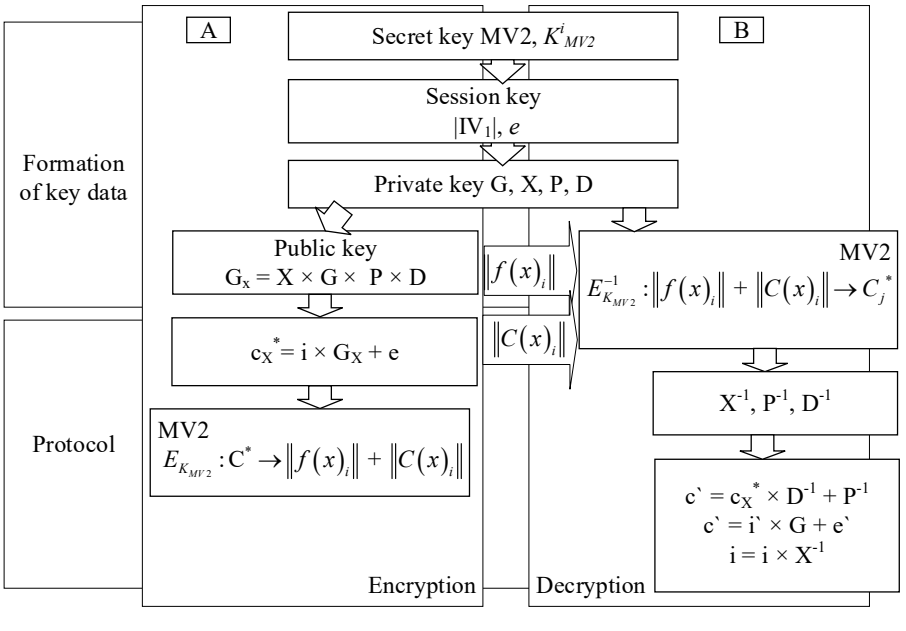

Fig. 2. Block diagram of McEliece's hybrid crypto-code construction on LDPC codes with damage

The mathematical model of McEliece's hybrid crypto-code construction uses the following input data:

– set of information resources $I = \{I_1, I_2, ... I_{q^k}\}$, for all $I_j \in GF(q)$.

– set of crypto-transformations to form a codeword on the generating matrix of the LDPC code:

$\varphi=(\varphi_1, \varphi_2, ..., \varphi_s)$, where $\phi_i : I \to C_{k-h_j}$, i=1, 2,..., s. where h_j – forms initialization vectors (V_1 – initialization vector, which determines the number and places of "puncture" of symbols in the codeword, V_2 – initialization vector, which determines the number and places of "adding" information symbols in the codeword);

– set of crypto transformations that allow to obtain the original information resource:

$$\phi^{-1}=\{\phi_1^{-1},\phi_2^{-1},...,\phi_s^{-1}\}, \text{ where } \phi_i^{-1}: C_{k-h_j} \to I;$$

– set of public keys:

$$KU_i=\{KU_1,KU_2,...,KU_S\}=\{G_1^{LDPC},G_2^{LDPC},...,G_S^{LDPC}\},$$

where $G_{X_{a_i}}^{LDPC_i}$ – generating matrix for the LDPC code. To generate the key let's use:

$$G_{X_{a_i}}^{LDPCu}=X^u \times G^{LDPCu} \times P^u, \ u \in \{1,2,...,s\};$$

– set of personal (private) user keys:

$$KR=\{KR_1,KR_2,...,KR_r\}=\{X^i,P^i,D^i\},$$

where the masking matrices: X^i – non-degenerate $k \times k$-matrix; P^i – permutative $n \times n$-matrix; D^i – diagonal $n \times n$-matrix. The diagonal matrix of the LDPC code is equal to the identity matrix, and cannot be used;

– a set of damaged texts ($C(x)_i$):

$$CFT=\{CFT_1,CFT_2,...,CFT_{q^k}\};$$

– a set of damage ($f(x)_i$ – flag):

$$CHD=\{CHD_1,CHD_2,...,CHD_{q^k}\};$$

– a set of formation of damaged text and damage (based on the algorithm key $MV2$) – $E=\{E_{K_{MV2}}^1,E_{K_{MV2}}^2,...,\phi_{K_{MV2}}^S\}$, $f(x)=n-|C(x)|$, if $|C(x)|>r$, where r – some parameter, $r \in_R Z_{q^m}, 0<r<n$;

– mapping set $MV2 \to F_n^r$, which defines a bijective mapping between a set of permutations $\{S_1,S_2,...,S_{2^n}\}$ and the set $\#F_n^r$, $\#F_n^r=\#\{(c,f)\}=2^n!$;

– a set of displaying damaged text into an information resource (based on the key – K_{MV2}^i, and algorithm $MV2$) – $E^{-1}=\{E_{K_{MV2}}^{1\ -1},E_{K_{MV2}}^{2\ -1},...,E_{K_{MV2}}^{S\ -1}\}$, where $E_{K_{MV2}}^{-1}: \|f(x)_i\| + \|C(x)_i\| \to I$.

The sender generates a code word: $C_j=M_i \times G_{X_{a_i}}^{LDPCu^T}+e$, where e – additional session key for each information parcel.

The $MV2$ algorithm receives a code word $C_j=M_i \times G_{X_{a_i}}^{LDPCu^T}+e$ and is converted in the $MV2$ algorithm into damaged text (remainder) and damage (flag):

$$E_{K_{MV2}}: C^* \to \|f(x)_i\| + \|C(x)_i\|.$$

The communication channel receives $\|f(x)_i\|$ and $\|C(x)_i\|$, in this case, transmission can be carried out either through one or two independent channels.

On the receiving side, the recipient uses the damage rule F_n^r, masking, the number and location of zero information symbols can decode the code word and receive an information message:

$$E_{K_{MV2}}^{-1}: \|f(x)_i\| + \|C(x)_i\| \to C_j^*,$$

$$I_i=\phi_u^{-1}(C_j^*,\{X,P,D\}_u).$$

When using an extended modified LDPC code, the recipient adds zero information symbols (along the initialization vector V_1), and also "receives" information symbols (according to the initialization vector V_2).

The masking matrices effect is removed from $C_j^*=C_j+C_{k-h_j}$:

$$C = C_j^* \times (P^u)^{-1} = \left(I_i \times (G_X^{LDPCu})^T + e\right) \times (P^u)^{-1} =$$

$$= \left(I_i \times (X^u \times G^{LDPC} \times P^u)^T + e\right) \times (P^u)^{-1} =$$

$$= I_i \times (X^u)^T \times (G^{LDPC})^T \times (P^u)^T \times (P^u)^{-1} + e \times (P^u)^{-1} =$$

$$= I_i \times (X^u)^T \times (G^{LDPC})^T + e \times (P^u)^{-1},$$

and then decodes the resulting vector using the Berlekamp-Massey algorithm [1, 2, 33]:

$$C = I_i \times (X^u)^T \times (G^{LDPC})^T + e \times (D^u)^{-1} \times (P^u)^{-1}.$$

Let's receive an information resource:

$$\left(I_i \cdot (X^u)^T\right) \times (X^u)^{-1} = I_i.$$

To ensure authenticity, the work proposes to use a modified UMAC algorithm on crypto-code constructions; the block diagram is shown in Fig. 3 [32].

In addition, it is proposed to use a modified SSL/TLS protocol on post-quantum algorithms. The protocol is proposed to use the synthesis of McEliece crypto-code constructions with the UMAC algorithm, in which the substrate is formed on the basis of the CCC [32]. The block diagram of the modified protocol is shown in Fig. 4. The proposed protocol provides the required level of security and allows to "eliminate" the identified "shortcomings" of the version 1.3 protocol. In addition, the use of various noise-resistant codes makes it possible to ensure the required level of security in the post-quantum period. To ensure various levels of information resources` security, it is proposed to use error-resistant codes with damage [33]. In Table 1 shows the results of studies of the relationship between time and the degree of secrecy of information, taking into account the classification of the security level. The results obtained confirm the possibility of using CCC on various codes in the post-quantum cryptoperiod.

Table 1

Relationship between time and degree of information secrecy

Security level	Quantum resistance	Noise-resistant codes
1	Strongest	*MEC*, flawed codes
2	Very strong	*MEC*
3	Stronger	*EC*
4	Strong	LDPC
5	Weak	Classic codes

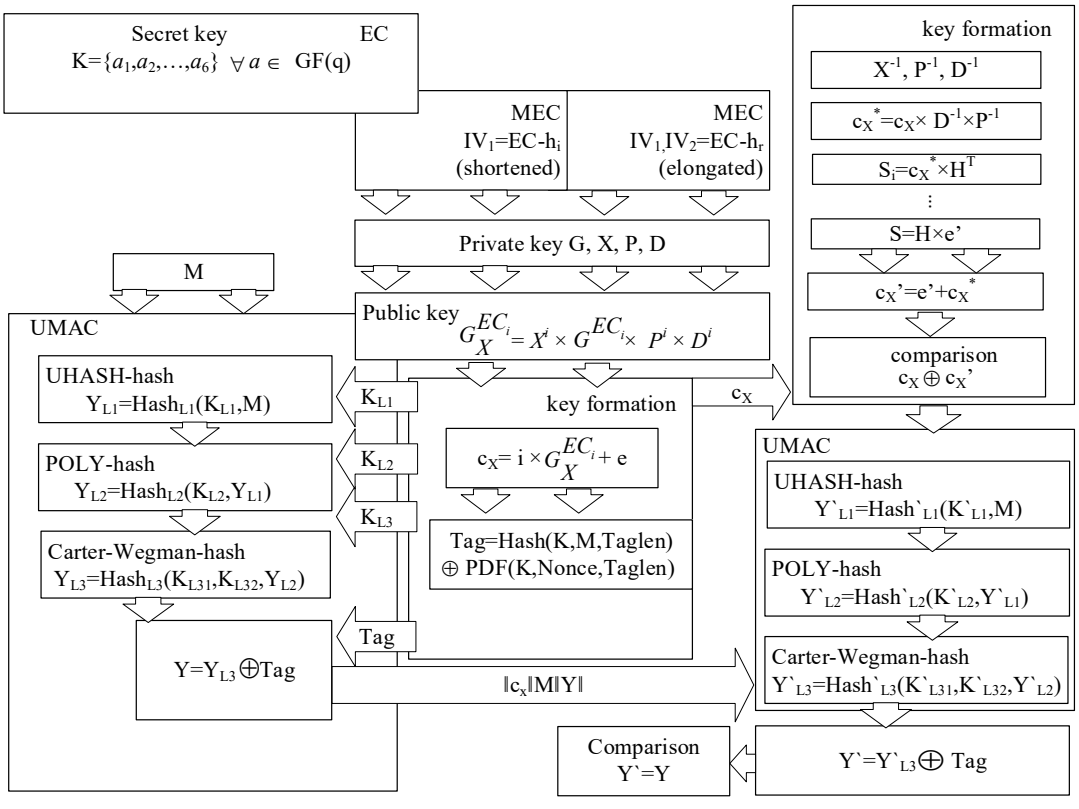

Fig. 3. Block diagram of a modified UMAC based on the McEliece crypto-code construction with modified (lengthened/shortened) codes

Table 2 presents the results of the ability to provide security services in the post-quantum period in wireless and mobile technology standards, taking into account the degree of security.

Table 2

Comparative characteristics of wireless and mobile Internet technologies

Technology	Security					
	Services					Level
	A_i^C	A_i^I	A_i^A	A_i^{Au}	A_i^{Inv}	
LTE (4G–6G)	–	–	+	–/+	–/+	5
IEEE 802.11ac (WiFi 5)	–	–	+	–/+	–/+	5
IEEE 802.11ax, Wi-Fi 6+KNX	–/+	–/+	+	–/+	–/+	5
IEEE 802.16+KNX	–/+	–/+	+	–/+	–/+	5
IEEE802.16m (WiMAX2)	–/+	–/+	+	–/+	–/+	5
Bluetooth 5+KNX	–/+	–/+	+	–/+	–/+	5
IEEE 802.15.4+KNX	–/+	–/+	+	–/+	–/+	4
CCC on classic-codes	–/+	–/+	+	+	+	5
CCC on LDPC-codes	+	+	+	+	+	4
CCC on EC	+	+	+	+	+	3
CCC on MEC	+	+	+	+	+	2
HCCC on EC (MEC)	+	+	+	+	+	1

Analysis of the Table 2 showed that to ensure security in socio-cyberphysical systems, it is proposed to use post-quantum algorithms, which, in contrast to modern security service mechanisms, make it possible to ensure the required level of cryptographic strength and efficiency.

The presented mathematical apparatus allows to estimate the main parameters of crypto-code structures on LDPC codes with damage and on modified codes.

The length of the plaintext (in bits) arriving at the input of a cryptosystem with unprofitable ones is determined by the following expressions:

– for HCCC on shortened LDPC-codes:

$$l_I = l_z^c + l_z^f,$$

where $l_z^c = K_c \times L + \frac{1}{K_f} \times s$ – damaged text length; $l_z^f = L + u \times s$ – length of damage; $s = \left[\frac{L_0 - L_{DT}}{L_{DT}}\right]$ – number of segments of flawed text; K_C=1–K_f≈0,758 – compression ratio of the remainder (flawed text) (at u=8, v=3, z=5); $K_f = \frac{2 - 2^{v-u+1}}{u} \approx 0.242$ –compression ratio flag (damage) (at u=8, v=3, z=5); $z = \frac{\log(u \times L) - 7}{\log(1/K_C)}$ – required for randomization of the *MV*2 algorithm, the number of permissible transformation rounds;

– for HCCC on lengthened LDPC-codes:

$$l_I = 1/2k \times m + l_z^c + l_z^f.$$

The length of the codogram (in bits) is determined by the following expressions:

– for HCCC on shortened LDPC-codes:

$$l_s = \left(2\sqrt{q} + q + 1 - 1/2k\right) \times \text{m}; \quad (1)$$

– for HCCC on lengthened LDPC-codes:

$$l_s = \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times m. \quad (2)$$

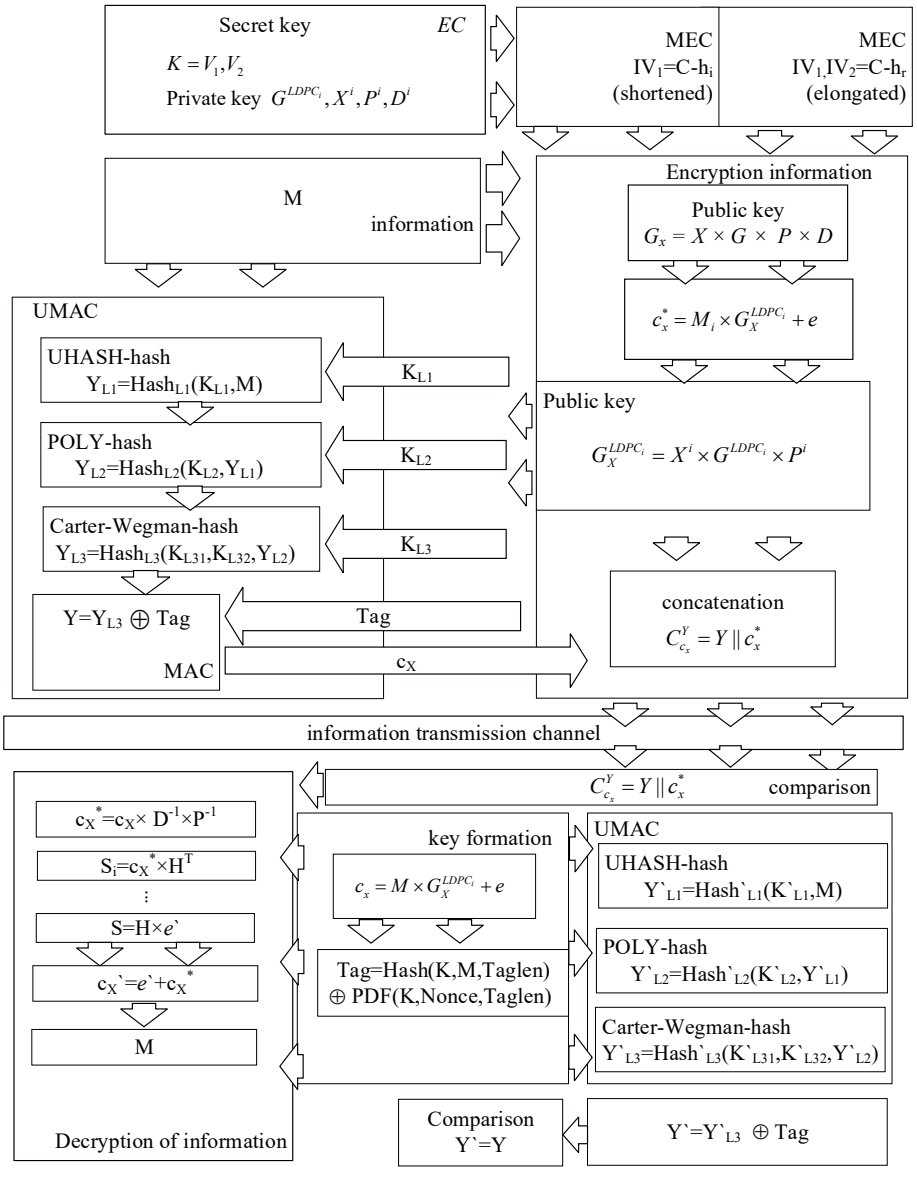

Fig. 4. Block diagram of the formation of an authenticated message based on crypto-code constructions on modified elliptic codes

Analysis of Tables 3, 4 and Fig. 5, 6 showed that the use of HCCC provides a significant reduction in the complexity of generating (≈12 times) and decoding (≈20 times) a cryptogram compared to the McEliece crypto-code construction on classical codes.

The length of the public key (in bits) is determined by the sum of the matrix elements G_X^{LDPC} and is specified by expressions:

– for HCCC on shortened LDPC-codes:

$$l_K = 1/2k \times \left(2\sqrt{q} + q + 1 - 1/2k\right) \times m; \quad (3)$$

– for HCCC on lengthened LDPC-codes:

$$l_K = 1/2k \times \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times m. \quad (4)$$

The length of the private key (in bits) is determined by the sum of the elements of the matrices X, P, D (in bits) and is given by the expressions:

– for HCCC on shortened LDPC-codes:

$$l_{K_+} = 1/2k\left\lceil \log_2\left(2\sqrt{q} + q + 1\right)\right\rceil + \left|F_u^v\right|, \quad (5)$$

where $\left|F_u^v\right| = 2^u!$ – power of a set of group transformations;

– for HCCC on lengthened LDPC-codes:

$$l_{K_+} = \left(1/2k - 1/2k\right)\left\lceil \log_2\left(2\sqrt{q} + q + 1\right)\right\rceil + \left|F_u^v\right|. \quad (6)$$

Due to the use of flawed codes in the McEliece HCCC, the required level of stability is ensured, which does not decrease with a decrease in the power of the Galois field. The level of resistance is provided by damage and the use of initialization vectors (when using shortened and/or extended LDPC codes).

The complexity of forming a codogram is determined by the expressions:

– for HCCC on shortened LDPC codes: when implementing systematic coding, it is determined by the expression:

$$O_K = (r+1) \times \left(2\sqrt{q} + q + 1 - 1/2k\right) + O\left(\frac{1 - K_C^u}{K_f} \times L\right); \quad (7)$$

for non-systematic coding:

$$O_K = O_K = (k+1)\times(k+1)\times$$
$$\times\left(2\sqrt{q}+q+1-1/2k\right)+O\left(\frac{1-K_C^u}{K_f}\times L\right); \quad (8)$$

– for HCCC on extended LDPC codes: when implementing systematic coding, it is determined by the expression:

$$O_K=(r+1)\times\begin{pmatrix}2\sqrt{q}+q+1-\\-1/2k+1/2k\end{pmatrix}+O\left(\frac{1-K_C^u}{K_f}\times L\right); \quad (9)$$

for non-systematic coding:

$$O_K=(k+1)\times\begin{pmatrix}2\sqrt{q}+q+1-\\-1/2k+1/2k\end{pmatrix}+O\left(\frac{1-K_C^u}{K_f}\times L\right). \quad (10)$$

The complexity of decoding a codogram is determined by the following expressions:

– HCCC on shortened LDPC-codes:

$$O_{SK} = 2\times\left(2\sqrt{q}+q+1-1/2k\right)^2+1/2k^2+$$
$$+4t^2+\left(t^2+t-2\right)^2/4+O\left(\frac{\alpha-z\times\log k}{\left|K_z^c\times L\right|}\right); \quad (11)$$

– HCCC on lengthened LDPC-codes:

$$O_{SK} = 2\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right)^2+$$
$$+k^2+4t^2+\left(t^2+t-2\right)^2/4+O\left(\frac{\alpha-z\times\log k}{\left|K_z^c\times L\right|}\right). \quad (12)$$

The complexity of the decoding process is determined by the expressions:

– for HCCC on shortened LDPC-codes:

$$O_{K+} = N_{\text{covering}}\times\left(2\sqrt{q}+q+1-1/2k\right)\times r+N_F \text{ or } (N_K), \quad (13)$$

where $N_F\approx\frac{K_C{}^z}{2^{1-K_C{}^{z+1}}}\times|F|$; K_C=97/128; $|F|$ – total length of output flags (damage) (bits) – with a known attacker of the remainder (damage text) and specified flags (damage), with an unknown key – $N_K\approx 2^{1190\times z}$; z=16;

– for HCCC on lengthened LDPC-codes:

$$O_{K+} = N_{\text{covering}}\times\left(2\sqrt{q}+q+1-1/2k+1/2k\right)\times$$
$$\times r+N_F \text{ or } (N_K). \quad (14)$$

The proposed mathematical apparatus allows not only to obtain various designs of LDPC codes, but also to form asymmetric crypto-code designs, which makes it possible to use them in the post-quantum period.

5. 2. Development of a block diagram of a methodology for constructing a multi-contour information security system in socio-cyberphysical systems

To construct a block diagram of the methodology for a multi-contour information system protection system, the following sequence of actions is proposed:

Stage 1. At this stage, a classification of threats is formed based on the set of threats into basic security services. This takes into account the properties of hybridity and synergy of threats, the possibility of their integration with social engineering methods, as well as their impact on the contours of each of the SCPS platforms [40]:

Internal contour of the information security system:

– 1st platform (social networks):

$$Q^{SS\ ISL}_{\text{hybrid}\,C,I,A,Au,Af\,synerg_{1\text{platform}}} =$$
$$=\left(Q^{SS\ ISL\ \ C}_{synerg_{1\text{platform}}}\cup\sum_{i=1}^{5}S_i^{\text{threats}}\times\alpha_i\right)\cap$$
$$\cap\left(Q^{SS\ ISL\ \ I}_{synerg_{1\text{platform}}}\cup\sum_{i=1}^{5}S_i^{\text{threats}}\times\alpha_i\right)\cap$$
$$\cap\left(Q^{SS\ ISL\ \ A}_{synerg_{1\text{platform}}}\cup\sum_{i=1}^{5}S_i^{\text{threats}}\times\alpha_i\right)\cap$$
$$\cap\left(Q^{SS\ ISL\ \ Au}_{synerg_{1\text{platform}}}\cup\sum_{i=1}^{5}S_i^{\text{threats}}\times\alpha_i\right)\cap$$
$$\cap\left(Q^{SS\ ISL\ \ Inv}_{synerg_{1\text{platform}}}\cup\sum_{i=1}^{5}S_i^{\text{threats}}\times\alpha_i\right), \quad (15)$$

where $Q^{SCS\ ISL}_{synerg_{1\text{platform}}}$ – synergy of threats to the corresponding security service; α_i – social engineering threat realization rate, $i\in\{0.25; 0.5; 0.75; 1.0\}$, where 0.25 – threat probability 1 time per year (low level); 0.5 – threat probability 1 time per month (medium level); 0.5 – threat probability 1 time per week (high level); 1.0 – threat probability 1 time per day (critical level).

– 2nd platform (cyberspace):

$$Q^{SCS\ ISL}_{\text{hybrid}\,C,I,A,Au,Af\,synerg_{2\text{platform}}} =$$
$$=\left(W^{SCS\ ISL\ \ s}_{synerg_{2\text{platform}}}\cup\sum_{i=1}^{5}S_i^{\text{threats}}\times\alpha_i\right)\cap$$
$$\cap\left(Q^{SCS\ ISL\ \ I}_{synerg_{2\text{platform}}}\cup\sum_{i=1}^{5}S_i^{\text{sthreats}}\times\alpha_i\right)\cap$$
$$\cap\left(Q^{SCS\ ISL\ \ A}_{synerg_{2\text{platform}}}\cup\sum_{i=1}^{5}S_i^{\text{sthreats}}\times\alpha_i\right)\cap$$
$$\cap\left(Q^{SCS\ ISL\ \ Au}_{synerg_{2\text{platform}}}\cup\sum_{i=1}^{5}S_i^{\text{sthreats}}\times\alpha_i\right)\cap$$
$$\cap\left(Q^{SCS\ ISL\ \ Inv}_{synerg_{2\text{platform}}}\cup\sum_{i=1}^{5}S_i^{\text{sthreats}}\times\alpha_i\right); \quad (16)$$

– 3rd platform (cyber-physical systems):

$$Q^{SCS\ ISL}_{\text{hybrid}\,C,I,A,Au,Af\,synerg_{3\text{platform}}} =$$
$$=\left(Q^{SCS\ ISL\ \ s}_{synerg_{3\text{platform}}}\cup\sum_{i=1}^{5}S_i^{\text{threats}}\times\alpha_i\right)\cap$$
$$\cap\left(Q^{SCS\ ISL\ \ I}_{synerg_{3\text{platform}}}\cup\sum_{i=1}^{5}S_i^{\text{sthreats}}\times\alpha_i\right)\cap$$
$$\cap\left(Q^{SCS\ ISL\ \ A}_{synerg_{3\text{platform}}}\cup\sum_{i=1}^{5}S_i^{\text{sthreats}}\times\alpha_i\right)$$
$$\cap\left(Q^{SCS\ ISL\ \ Au}_{synerg_{3\text{platform}}}\cup\sum_{i=1}^{5}S_i^{\text{sthreats}}\times\alpha_i\right)\cap$$
$$\cap\left(Q^{SCS\ ISL\ \ Inv}_{synerg_{3\text{platform}}}\cup\sum_{i=1}^{5}S_i^{\text{sthreats}}\times\alpha_i\right). \quad (17)$$

Overall assessment of threats to the internal contour for all platforms:

$$Q_{ISL}^{SCS} = W_{\text{hybrid } C,I,A,Au,Af\ synerg_{1\text{platform}}}^{SCS\ ISL} \cup$$
$$\cup Q_{\text{hybrid } C,I,A,Au,Af\ synerg_{2\text{platform}}}^{SCS\ ISL} \cup$$
$$\cup Q_{\text{hybrid } C,I,A,Au,Af\ synerg_{3\text{platform}}}^{SCS\ ISL}. \quad (18)$$

External contour of the information security system:
– 1st platform (social networks):

$$Q_{\text{hybrid } C,I,A,Au,Af\ synerg_{1\text{platform}}}^{SCS\ ESL} =$$
$$= \left(Q_{synerg_{1\text{platform}}}^{SCS\ ESL\ \ s} \cup \sum_{i=1}^{5} S_i^{\text{threats}} \times \alpha_i \right) \cap$$
$$\cap \left(Q_{synerg_{1\text{platform}}}^{SS\ ESL} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i \right)^{I} \cap$$
$$\cap \left(Q_{synerg_{1\text{platform}}}^{SCS\ ESL} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i \right)^{I} \cap$$
$$\cap \left(Q_{synerg_{1\text{platform}}}^{SCS\ ESL\ \ A} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i \right) \cap$$
$$\cap \left(Q_{synerg_{1\text{platform}}}^{SCS\ ESL\ \ Au} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i \right) \cap$$
$$\cap \left(Q_{synerg_{1\text{platform}\,\partial}}^{SCS\ ESL\ \ Inv} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i \right); \quad (19)$$

– 2nd platform (cyberspace):

$$Q_{\text{hybrid } C,I,A,Au,Af\ synerg_{2\text{platform}}}^{SCS\ ESL} =$$
$$= \left(Q_{synerg_{2\text{platform}}}^{SCS\ ESL\ \ C} \cup \sum_{i=1}^{5} S_i^{\text{threats}} \times \alpha_i \right) \cap$$
$$\cap \left(Q_{synerg_{2\text{platform}}}^{SCS\ ESL\ \ I} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i \right) \cap$$
$$\cap \left(Q_{synerg_{2\text{platform}}}^{SCS\ ESL\ \ A} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i \right) \cap$$
$$\cap \left(Q_{synerg_{2\text{platform}}}^{SCS\ ESL\ \ Au} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i \right) \cap$$
$$\cap \left(Q_{synerg_{2\text{platform}}}^{SCS\ ESL\ \ Inv} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i \right); \quad (20)$$

– 3rd platform (cyber-physical systems):

$$Q_{\text{hybrid } C,I,A,Au,Af\ synerg_{3\text{platform}}}^{SCS\ ESL} =$$
$$= \left(Q_{synerg_{3\text{platform}}}^{SCS\ ESL\ \ s} \cup \sum_{i=1}^{5} S_i^{\text{threats}} \times \alpha_i \right) \cap$$
$$\cap \left(Q_{synerg_{3\text{platform}}}^{SCS\ ESL\ \ I} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i \right) \cap$$
$$\cap \left(Q_{synerg_{3\text{platform}}}^{SCS\ ESL\ \ A} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i \right) \cap$$
$$\cap \left(Q_{synerg_{3\text{platform}}}^{SCS\ ESL\ \ Au} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i \right) \cap$$
$$\cap \left(Q_{synerg_{3\text{platform}}}^{SCS\ ESL\ \ Inv} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i \right). \quad (21)$$

The overall assessment of threats to the external contour for all platforms is:

$$Q_{ESL}^{SCS} = Q_{\text{hybrid } C,I,A,Au,Af\ synerg_{1\text{platform}}}^{SCS\ ESL} \cup$$
$$\cup Q_{\text{hybrid } C,I,A,Au,Af\ synerg_{2\text{platform}}}^{SCS\ ESL} \cup$$
$$\cup Q_{\text{hybrid } C,I,A,Au,Af\ synerg_{3\text{platform}}}^{SCS\ ESL}. \quad (22)$$

The general assessment of threats to a multi-contour information protection system is determined:

$$Q_{\text{final}}^{CPSS} = Q_{ISL}^{CPSS} \cup Q_{ESL}^{CPSS}. \quad (23)$$

Stage 2. Assessment (if data is available) of the socio-political and economic state of the society (region). For this purpose, the approach in [42] is used.

A mathematical model for assessing the exposure to social influence of elements of state institutions, media and informal leaders on regional communities:

$$\mathbf{IMP} = \mathbf{AA} \cup \mathbf{IL} \cup \mathbf{MM} \cup \mathbf{PP},$$

where matrix **IMP** – generalized matrix of the influence of various institutions on the corresponding age groups of the regional community [42]:

$$\mathbf{IMP} = \begin{pmatrix} \mathbf{AA} \\ \mathbf{IL} \\ \mathbf{MM} \\ \mathbf{PP} \end{pmatrix} = \begin{pmatrix} \eta_{11} \cdot \sigma_1 & \dots & \eta_{14} \cdot \sigma_4 \\ \dots & \dots & \dots \\ \eta_{k1} \cdot \sigma_1 & \dots & \eta_{k4} \cdot \sigma_4 \\ \mu_{k+1,1} \cdot \sigma_1 & \dots & \mu_{k+1,1} \cdot \sigma_4 \\ \dots & \dots & \dots \\ \mu_{k+l,1} \cdot \sigma_1 & \dots & \mu_{k+l,1} \cdot \sigma_4 \\ \rho_{k+l+1,4} & \dots & \rho_{k+l+1,4} \\ \dots & \dots & \dots \\ \rho_{k+l+m,4} & \dots & \rho_{k+l+m,4} \\ \theta_{k+l+m+1,1} \cdot \sigma_1 & \dots & \theta_{k+l+m+1,4} \cdot \sigma_4 \\ \dots & \dots & \dots \\ \theta_{k+l+m+n,1} \cdot \sigma_1 & \dots & \theta_{k+l+m+n,4} \cdot \sigma_4 \end{pmatrix}, \quad (24)$$

where $\mathbf{AA} = \begin{pmatrix} \eta_{1,1} & \dots & \eta_{1,4} \\ \dots & \dots & \dots \\ \eta_{k,1} & \dots & \eta_{k,4} \end{pmatrix}$ – influence of formal leaders;

$\mathbf{IL} = \begin{pmatrix} \mu_{1,1} & \dots & \mu_{1,4} \\ \dots & \dots & \dots \\ \mu_{l,1} & \dots & \mu_{l,4} \end{pmatrix}$ – influence of informal leaders;

$\mathbf{MM} = \begin{pmatrix} \rho_{1,1} & \dots & \rho_{1,4} \\ \dots & \dots & \dots \\ \rho_{m,1} & \dots & \rho_{m,4} \end{pmatrix}$ – influence of mass media;

$\mathbf{PP} = \begin{pmatrix} \theta_{1,1} & \dots & \theta_{1,4} \\ \dots & \dots & \dots \\ \theta_{k,1} & \dots & \theta_{k,4} \end{pmatrix}$. – influence of political parties [42].

Stage 3. Assessment of the ratio of threats to the number of attackers ("predators") and infrastructure elements of socio-cyberphysical systems ("victims") based on the approach in [53, 54]:

– model 1. Computing capabilities and targeting of cyber-attacks:

$$A_1^{SCS}=\begin{cases}\dfrac{dN_1}{dt}=\left(\arg\max\limits_{\forall Tr_j\in Tr_C^D}K_l^D\times K_l^A\right)\times\\ \times\left(\sum\limits_{i=1}^{Q}\begin{pmatrix}N_{1_i}^C\times A_i^C+N_{1_i}^I\times A_i^I+N_{1_i}^A\times A_i^A+\\ +N_{1_i}^{Au}\times A_i^{Au}+N_{1_i}^{Aff}\times A_i^{Aff}\end{pmatrix}\right)-\\ -\left(\sum\limits_{i=1}^{M}\begin{pmatrix}w_{SCSi}{}^C\cap w_{SCSi}{}^I\cap w_{SCSi}{}^A\cap\\ \cap w_{SCSi}{}^{Au}\cap w_{SCSi}{}^{Aff}\end{pmatrix}\chi_i^{SCS}\right)\tilde{N}_1\times\\ \times\left(N_2\times\left|W_{\text{hybrid }C,I,A,Au,Af\,synerg}\right|\right);\\ \dfrac{dN_2}{dt}=-\left(\dfrac{1}{M}\sum\limits_{i=1}^{M}\nu_i\times p_{rj}\times r_{motiv}\right)\widetilde{N}_2+\\ +\left(\dfrac{1}{KB}\sum\limits_{k=1}^{K}\sum\limits_{g=1}^{B}\left(\mu_{kg}^l\times w_{kg}^l\right)\right)\widetilde{N}_2\widetilde{N}_1,\end{cases}\quad(25)$$

where $\tilde{N}_1=\sum\limits_{i=1}^{Q}\begin{pmatrix}N_{1_i}^C\times A_i^C+N_{1_i}^I\times A_i^I+N_{1_i}^A\times A_i^A+\\ +N_{1_i}^{Au}\times A_i^{Au}+N_{1_i}^{Aff}\times A_i^{Aff}\end{pmatrix}$ – number of attack targets; $\widetilde{N}_2=N_2\times\left|W_{\text{hybrid }C,I,A,Au,Af\,synerg}\right|$ – change in the number of threats on SCPS, where:

$$W_{\text{hybrid }C,I,A,Au,Af\,synerg}=W_{synerg}^C\cap W_{synerg}^I\cap W_{synerg}^A\cap$$
$$\cap W_{synerg}^{Au}\cap W_{synerg}^{Aff},$$

$$W_{\text{hybrid }C,I,A,Au,Af\,synerg}=W_{synerg}^C\cap W_{synerg}^I\cap W_{synerg}^A\cap$$
$$\cap W_{synerg}^{Au}\cap W_{synerg}^{Aff},$$

The calculation of individual components is given in the work [42].

The model provides the formation of a classifier of threats and attackers, as well as their relationship. This approach forms the point of irreversibility, at which the "impossibility" of carrying out a targeted attack is determined.

Model 2 takes into account the "interest" of criminals and/or cyber groups in carrying out a targeted attack, their motivation and competition:

– model 2. Possible competition of attackers [42]:

$$A_2^{SCS}=\begin{cases}\dfrac{dN_1}{dt}=\left(\arg\max\limits_{\forall Tr_j\in Tr_C^D}K_l^D\times K_l^A\right)\times\\ \times\left(\sum\limits_{i=1}^{Q}\begin{pmatrix}N_{1_i}^C\times A_i^C+N_{1_i}^I\times A_i^I+N_{1_i}^A\times A_i^A+\\ +N_{1_i}^{Au}\times A_i^{Au}+N_{1_i}^{Aff}\times A_i^{Aff}\end{pmatrix}\right)-\\ -\left(\sum\limits_{i=1}^{M}\begin{pmatrix}w_{SCSi}{}^C\cap w_{SCSi}{}^I\cap w_{SCSi}{}^A\cap\\ \cap w_{SCSi}{}^{Au}\cap w_{SCSi}{}^{Aff}\end{pmatrix}\chi_i^{SCS}\right)\times\\ \times\tilde{N}_1\left(\widetilde{N_2^1}\cap\widetilde{N_2^2}\cap\ldots\cap\widetilde{N_2^w}\right);\\ \dfrac{dN_2}{dt}=-\left(\dfrac{1}{M}\sum\limits_{i=1}^{M}\nu_i\times p_{rj}\times r_{motiv}\right)\times\\ \times\left(\widetilde{N_2^1}\cap\widetilde{N_2^2}\cap\ldots\cap\widetilde{N_2^w}\right)+\\ +\left(\dfrac{1}{KB}\sum\limits_{k=1}^{K}\sum\limits_{g=1}^{B}\left(\mu_{kg}^l\times w_{kg}^l\right)\right)\times\\ \times\left(\widetilde{N_2^1}\cap\widetilde{N_2^2}\cap\ldots\cap\widetilde{N_2^w}\right)\widetilde{N}_1,\end{cases}\quad(26)$$

where the number of "predators" belongs to the plural $\left\{\widetilde{N_2^j}\right\}, j\in 1,\ldots Q.$

The model provides the computing capabilities of attackers and the vector of technology development:

– model 3. Opportunities for grouping attackers/cyber groups to achieve the goals of a cyber-attack [42]:

$$A_3^{SCS}=\begin{cases}\dfrac{dN_1}{dt}=\left(\arg\max\limits_{\forall Tr_j\in Tr_C^D}K_l^D\times K_l^A\right)\times\\ \times\left(\sum\limits_{i=1}^{Q}\begin{pmatrix}N_{1_i}^C\times A_i^C+N_{1_i}^I\times A_i^I+N_{1_i}^A\times A_i^A+\\ +N_{1_i}^{Au}\times A_i^{Au}+N_{1_i}^{Aff}\times A_i^{Aff}\end{pmatrix}\right)-\\ -\left(\sum\limits_{i=1}^{M}\begin{pmatrix}w_{SCSi}{}^C\cap w_{SCSi}{}^I\cap w_{SCSi}{}^A\cap\\ \cap w_{SCSi}{}^{Au}\cap w_{SCSi}{}^{Aff}\\ \times\chi_i^{SCS}\end{pmatrix}\times\right)\times\\ \times\tilde{N}_1\left(\widetilde{\sum\limits_{j=1}^{w}N_2^w}\right);\\ \dfrac{dN_2}{dt}=-\left(\dfrac{1}{M}\sum\limits_{i=1}^{M}\nu_i\times p_{rj}\times r_{motiv}\right)\left(\widetilde{\sum\limits_{j=1}^{w}N_2^w}\right)+\\ +\left(\dfrac{1}{KB}\sum\limits_{k=1}^{K}\sum\limits_{g=1}^{B}\left(\mu_{kg}^l\times w_{kg}^l\right)\right)\times\left(\widetilde{\sum\limits_{j=1}^{w}N_2^w}\right)\widetilde{N}_1.\end{cases}\quad(27)$$

The model takes into account the financial capabilities of cyber groups (attackers), their political and social motivations for implementing threats:

– model 4. Relationships between "prey" species and "predator" species [42]:

$$A_4^{SCS}=\begin{cases}\dfrac{dN_1}{dt}=\left(\arg\max\limits_{\forall Tr_j\in Tr_C^D}K_l^D\times K_l^A\right)\times\\ \times\left(\sum\limits_{i=1}^{Q}\begin{pmatrix}N_{1_i}^C\times A_i^C+N_{1_i}^I\times A_i^I+N_{1_i}^A\times A_i^A+\\ +N_{1_i}^{Au}\times A_i^{Au}+N_{1_i}^{Aff}\times A_i^{Aff}\end{pmatrix}\right)-\\ -\left(\sum\limits_{i=1}^{M}\begin{pmatrix}w_{SCSi}{}^C\cap w_{SCSi}{}^I\cap w_{SCSi}{}^A\cap\\ \cap w_{SCSi}{}^{Au}\cap w_{SCSi}{}^{Aff}\\ \times\chi_i^{SCS}\end{pmatrix}\times\right)\times\\ \times\tilde{N}_1\left(\widetilde{\sum\limits_{j=1}^{w}N_2^w}\right)-\varepsilon\widetilde{N_1}^2;\\ \dfrac{dN_2}{dt}=-\left(\dfrac{1}{M}\sum\limits_{i=1}^{M}\nu_i\times p_{rj}\times r_{motiv}\right)\left(\widetilde{\sum\limits_{j=1}^{w}N_2^w}\right)+\\ +\left(\dfrac{1}{KB}\sum\limits_{k=1}^{K}\sum\limits_{g=1}^{B}\left(\mu_{kg}^l\times w_{kg}^l\right)\right)\left(\widetilde{\sum\limits_{j=1}^{w}N_2^w}\right)\widetilde{N}_1-\xi\widetilde{N_2}^2,\end{cases}\quad(28)$$

where coefficients ε, $\zeta>0$ – harming the "prey" and "predator" respectively [42].

The proposed models practically allow to take into account the modern financial computing capabilities of attackers.

Stage 4. Assessment of the integrated indicator of the current security level of a multi-contour protection system.

Stage 5. Modification of security service mechanisms in a multi-contour information security system (integration of post-quantum algorithms). Using post-quantum algorithms to provide essential security services. Fig. 5, 6 show a block diagram of the methodology for constructing a multi-contour information security system. The main difference from known approaches is the possibility of synthesizing both expert and system analysis of not only targeted threats to socio-cyberphysical systems, but also

the possibility of objectively assessing the current state of information security. This approach allows to respond in a timely manner to possible changes (modifications) of targeted threats, as well as take into account their synergy and hybridity, and the possibility of combining them with social engineering methods. The proposed practical solutions for providing security services based on post-quantum algorithms make it possible to ensure the required level of security of confidential information with different levels of secrecy.

To assess the integrated security indicator, it is proposed to use an assessment software package [39], as well as the proposed methodology and limitations:

1st Step. Formation of expert assessments of threats, their impact on security services, the possibility of signs of synergy and hybridity, as well as the integration of social engineering methods. Determine the impact of the threat on the infrastructure layer (ISO/OSI models). In this case, a matrix of weighting coefficients is formed:

$$S^*_{\text{sthreats}} = \left\| S_{\text{sthreats}_{ij}} \right\|,$$

where i – security services, j – corresponding threat, $j \in \overline{\forall 1 \ldots N}$.

2nd Step. Formation of a matrix of correspondence between information resources and security services: $S^*_{\text{inf}} = \left\| S_{\text{inf}_{il}} \right\|$, where i – security services, l – information resource, $l \in \overline{\forall 1 \ldots L}$. When filling out the matrix, the need to provide an appropriate security service is taken into account (1 – service, 0 – service is not needed).

3rd Step. Forming a dependency between information resources and infrastructure levels (ISO/OSI models) where information circulates and/or is stored:

$$S^*_{\text{ISO}} = \left\| S_{ISO_{kl}} \right\|,$$

where k – presence and type of connection, infrastructure element (level) where information is stored, l – information resource, $l \in \overline{\forall 1 \ldots L}$.

4th Step. Formation of dependence of threats and information resources (assessment of infrastructure criticality):

$$S^*_{\text{inf/sthreats}} = \left\| S_{\text{inf}_{lj}} \right\|,$$

where l – information resource, $l \in \overline{\forall 1 \ldots L}$. j – corresponding threat, $j \in \overline{\forall 1 \ldots N}$. This step allows to determine the criticality of unauthorized access to a particular information resource.

5th Step. Formation of dependency between threats and infrastructure elements (ISO/OSI model level):

$$S^*_{\text{sthreats}/ISO} = \left\| S_{\text{sthreats}/ISO_{kj}} \right\|,$$

where k – presence and type of communication, infrastructure element (level) where information is stored, j – corresponding threat, $j \in \overline{\forall 1 \ldots N}$. The step allows to identify critical points in the infrastructure and determine preventive security measures in advance.

6th Step. Formation of an assessment of the security of a socio-cyberphysical system based on the analysis of Steps 2 and 3 (finding the connection between information resources, infrastructure elements (critical points of unauthorized access/information leakage) and security services).

7th Step. Forming an assessment of the capabilities of the current information security system to counter threats:

$$S^*_{\text{sthreats/protection system}} = \left\| S_{\text{sthreats/protection system}_{qj}} \right\|,$$

where q – the presence of a mechanism to counter the threat, j – corresponding threat, $j \in \overline{\forall 1 \ldots N}$.

8th Step. Formation of assessment of regulators and legislative acts.

9th Step. Formation of an assessment of the current state of the security system. This takes into account the results of steps 7–9.

The presented methodology uses the following requirements.

After calculating the key compliance matrices, it is necessary to determine the synergistic effect of the interaction of cybersecurity components (security services, information resources and infrastructure elements).

For the correspondence matrix between security services and information resources:

$$S^*_{\text{inf}} = \left\| S_{\text{inf}_{il}} \right\|,$$

where i – security services, l – information resource.

After calculating the matrix, the level of importance of each service is determined $\left(S_{\text{inf}_i}\right)$ and each resource $\left(S_{\text{inf}_l}\right)$, where i=1,...,5, l=1,...,8, by formulas:

$$S_{\text{inf}_i} = \sum_{l=1}^{8} S_{\text{inf}_{il}}, \quad S_{\text{inf}_l} = \sum_{i=1}^{5} S_{\text{inf}_{il}}. \tag{29}$$

After this, the total levels of service importance are determined $\left(S_{\text{inf}_i s}\right)$ and resources $\left(S_{\text{inf}_l s}\right)$ by formulas:

$$S_{\text{inf}_i s} = \sum_{i=1}^{5} S_{\text{inf}_i}, \quad S_{\text{inf}_l s} = \sum_{l=1}^{8} S_{\text{inf}_l}. \tag{30}$$

The following determines the weighting coefficients for services $\left(\alpha S_{\text{inf}_i}\right)$ and resources $\left(\alpha S_{\text{inf}_l}\right)$ by formulas:

$$\alpha S_{\text{inf}_i} = \frac{S_{\text{inf}_i}}{S_{\text{inf}_i s}},$$

where i=1, ..., 5;

$$\alpha S_{\text{inf}_l} = \frac{S_{\text{inf}_l}}{S_{\text{inf}_l s}}, \tag{31}$$

where l=1,...,8.

Services and resources are then ranked according to certain weights from largest to smallest to determine the most significant services/resources according to their interaction matrix.

Next, an integral indicator of the current security level is formed for the correspondence matrix between security services and information resources. For this purpose, the absolute and relative value of the integral indicator is determined:

$$IS_{\text{inf}\_abs} = \frac{\sum S_{\text{inf}_{il}}}{i \times l},$$

$$IS_{\text{inf}\_rel} = \frac{IS_{\text{inf}\_abs} - S_{\text{inf}_{il}\min}}{S_{\text{inf}_{il}\max} - S_{\text{inf}_{il}\min}}, \tag{32}$$

where IS_{inf_abs} – absolute integral indicator of the current level of information security for the compliance matrix of security services and information resources; IS_{inf_rel} – relative integral indicator of the current level of information security for the compliance matrix of security services and information resources; $S_{inf_{il}}$ – elements of the general matrix of compliance between security services and information resources; i – number of security services; l – number of information resources; $S_{inf_{ij}\,min}$ – minimum element of the compliance matrix between security services and information resources; $S_{inf_{ij}\,max}$ – minimum element of the matrix of compliance between security services and information resources.

For a dependency matrix between information resources and infrastructure layers (ISO/OSI models) where information circulates and/or is stored:

$$S^{*}_{ISO} = \left\| S_{ISO_{kl}} \right\|,$$

where k – presence and type of connection, infrastructure element (level) where information is stored, l – information resource.

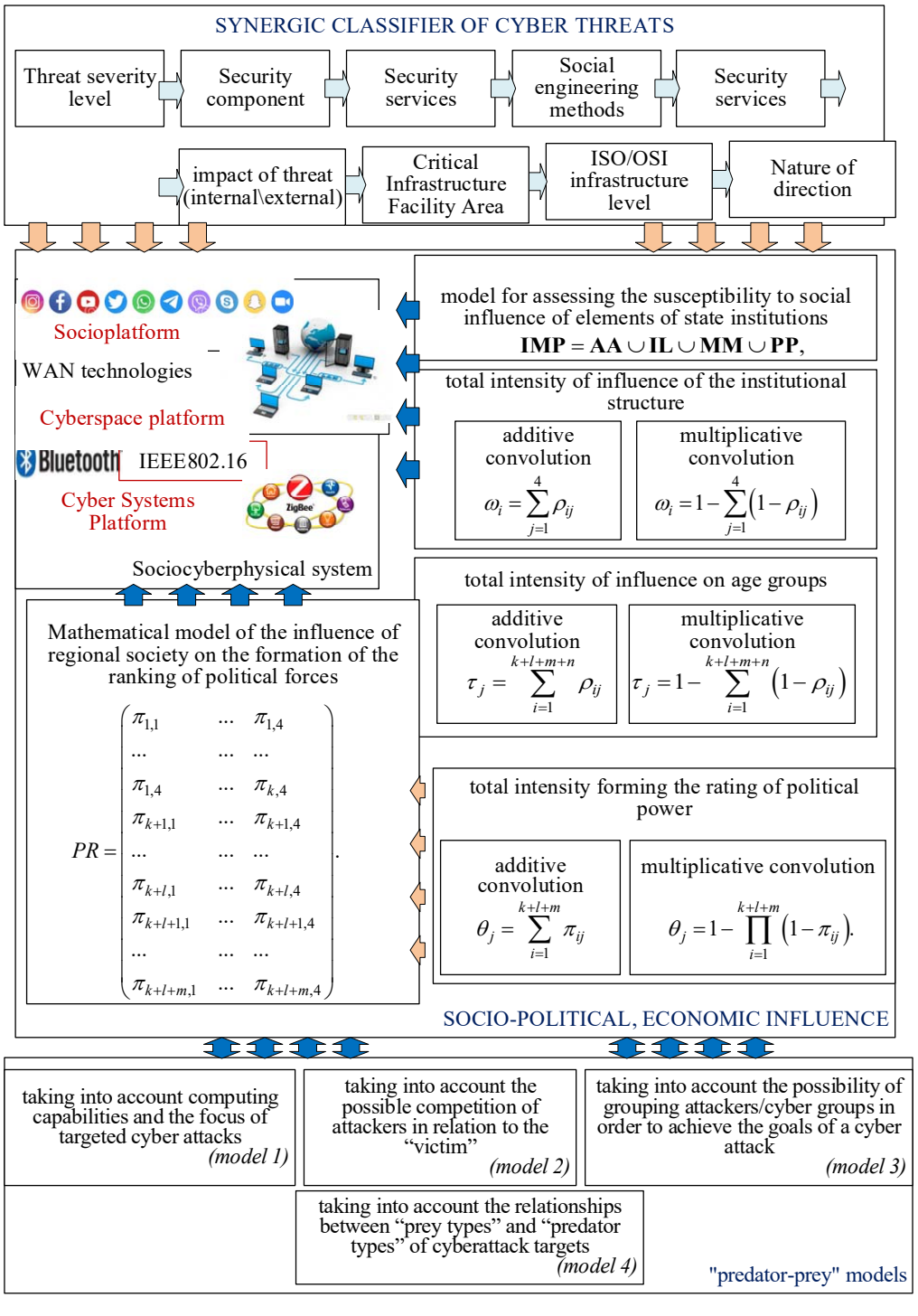

Fig. 5. Block diagram of constructing a system for assessing the current state of a multi-contour protection system

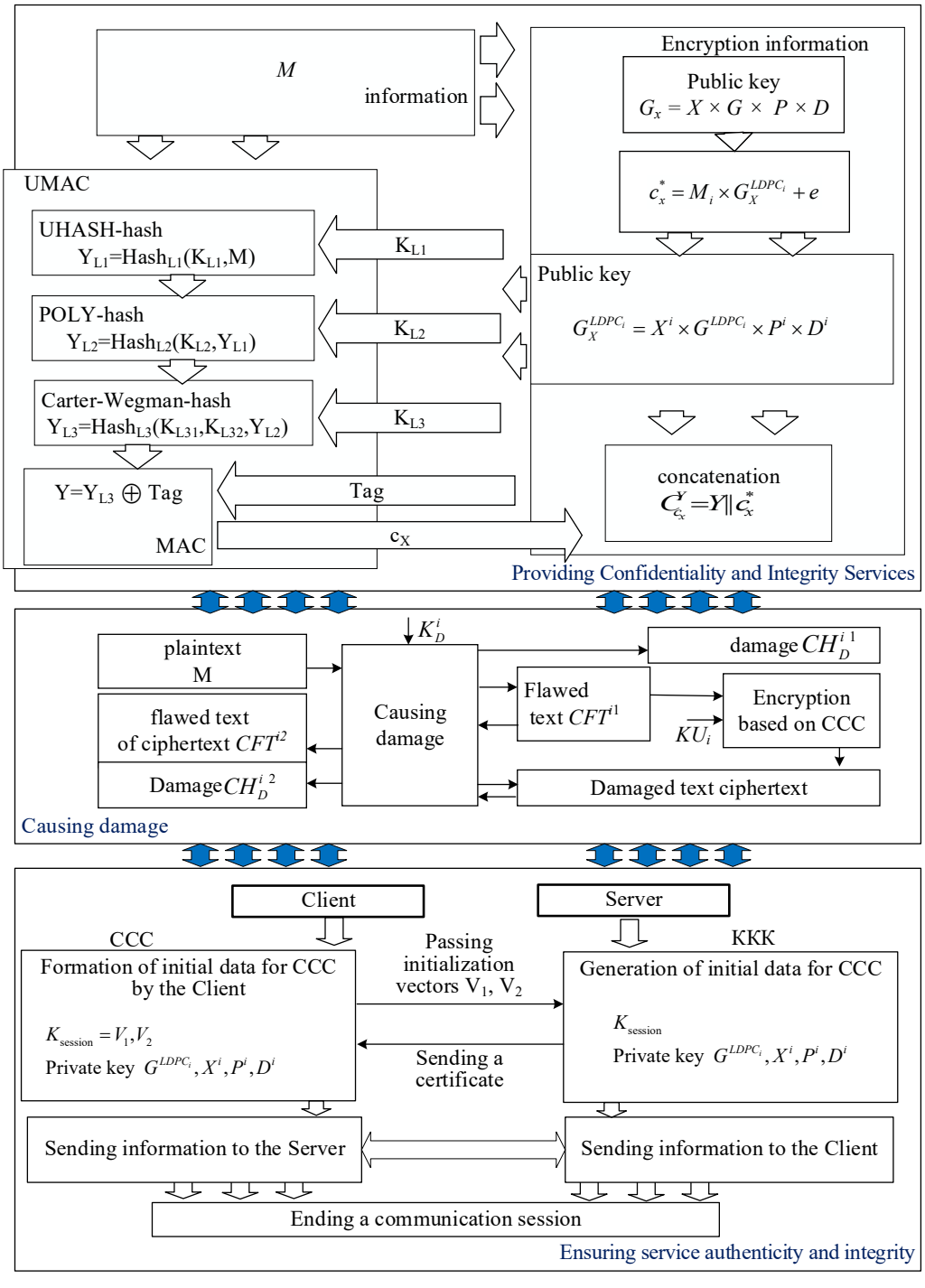

Fig. 6. Block diagram of mechanisms for providing security services in multi-contour information security systems

After calculating the matrix, the level of importance of each information resource is determined $\left(S_{ISO_k}\right)$ and each level of infrastructure $\left(S_{ISO_l}\right)$, where k=1,...,8, l=1,...,7, by formulas:

$$S_{ISO_k} = \sum_{l=1}^{7} S_{ISO_{kl}}, \quad S_{ISO_l} = \sum_{k=1}^{8} S_{ISO_{kl}}. \tag{33}$$

After this, the total levels of information resources are determined $\left(S_{ISO_k s}\right)$ and infrastructure levels $\left(S_{ISO_l s}\right)$ by formulas:

$$S_{ISO_k s} = \sum_{k=1}^{8} S_{ISO_k}, \quad S_{ISO_l s} = \sum_{l=1}^{7} S_{ISO_l}. \tag{34}$$

The following determines the weighting coefficients for resources $\left(\alpha S_{ISO_k}\right)$ and infrastructure levels $\left(\alpha S_{ISO_l}\right)$ by formulas:

$$\alpha S_{ISO_k} = \frac{S_{ISO_k}}{S_{ISO_k s}},$$

where k=1,...,8;

$$\alpha S_{ISO_l} = \frac{S_{ISO_l}}{S_{ISO_l s}}, \tag{35}$$

where l=1, ..., 7.

The resources and layers of infrastructure are then ranked according to certain weighting factors from largest to smallest to determine the most significant resources/layers in accordance with the matrix of their interactions.

Next, an integral indicator of the current security level is formed for the correspondence matrix between information resources and infrastructure levels. For this purpose, the absolute and relative value of the integral indicator is determined:

$$IS_{ISO\_abs} = \frac{\sum S_{ISO_{kl}}}{k \times l}, \quad IS_{ISO\_rel} = \frac{IS_{ISO\_abs} - S_{ISO_{kl}\min}}{S_{ISO_{kl}\max} - S_{ISO_{kl}\min}}, \qquad (36)$$

where IS_{ISO_abs} – absolute integral indicator of the current level of information security for the correspondence matrix between information resources and infrastructure levels; IS_{ISO_rel} – relative integral indicator of the current level of information security for the correspondence matrix between information resources and infrastructure levels; $S_{ISO_{kl}}$ – elements of the general matrix of correspondence between information resources and infrastructure levels; k – number of information resources; l – number of infrastructure levels; $S_{ISO_{kl}\min}$ – the minimum element of the correspondence matrix between information resources and infrastructure levels; $S_{ISO_{kl}\max}$ – the minimum element of the correspondence matrix between information resources and infrastructure levels.

For the mapping matrix between security services and infrastructure layers: $S^*_{serv} = \left\| S_{serv_{ij}} \right\|$, where i – security service, l – infrastructure level.

After calculating the matrix, the level of importance of each service is determined $\left(S_{serv_i}\right)$ and each level of infrastructure $\left(S_{serv_l}\right)$, where i=1,...,5, l=1,...,7, by formulas:

$$S_{serv_i} = \sum_{l=1}^{7} S_{serv_{il}}, \quad S_{serv_l} = \sum_{i=1}^{5} S_{serv_{il}}. \qquad (37)$$

After this, the total levels of service importance are determined $\left(\alpha S_{serv_i}\right)$ and infrastructure levels $\left(S_{\inf_l s}\right)$ by formulas:

$$S_{serv_i s} = \sum_{i=1}^{5} S_{serv_i}, \quad S_{serv_l s} = \sum_{l=1}^{7} S_{serv_l}. \qquad (38)$$

Next determined the weighting coefficients for services $\left(\alpha S_{serv_i}\right)$ and infrastructure levels $\left(\alpha S_{serv_l}\right)$ by formulas:

$$\alpha S_{serv_i} = \frac{S_{serv_i}}{S_{serv_i s}},$$

where i=1,...,5;

$$\alpha S_{serv_l} = \frac{S_{serv_l}}{S_{serv_l s}}, \qquad (39)$$

where l=1,...,7.

Services and resources are then weighted from largest to smallest to determine the most significant services/infrastructure layers according to their interaction matrix.

Next, an integral indicator of the current security level is formed for the correspondence matrix between security services and infrastructure levels. For this purpose, the absolute and relative value of the integral indicator is determined:

$$IS_{serv\_abs} = \frac{\sum S_{serv_{il}}}{i \times l},$$

$$IS_{serv\_rel} = \frac{IS_{serv\_abs} - S_{serv_{il}\min}}{S_{serv_{il}\max} - S_{serv_{il}\min}}, \qquad (40)$$

where IS_{serv_abs} – absolute integral indicator of the current level of information security for the correspondence matrix of security services and infrastructure levels; IS_{serv_rel} – relative integral indicator of the current level of information security for the matrix of correspondence between security services and infrastructure levels; $S_{serv_{il}}$ – elements of the general matrix of correspondence between security services and infrastructure levels; $S_{serv_{il}\min}$ – minimum element of the matrix of correspondence between security services and infrastructure levels.

The general integral indicator of the current level of information security in the analyzed security system is formed by additive convolution of individual absolute integral indicators and multiplicative convolution of individual relative integral indicators.

The additive integral indicator of the current level of information security in the security system is calculated using the formula:

$$IS_{add} = IS_{\inf\_abs} + IS_{ISO\_abs} + IS_{serv\_abs}. \qquad (41)$$

The multiplicative integral indicator of the current level of information protection in the security system is calculated using the formula:

$$IS_{mult} = IS_{\inf\_rel} + IS_{ISO\_rel} + IS_{serv\_rel}. \qquad (42)$$

In this way, it is possible to determine the overall integral assessment of the security of the system: the closer the value of the relative indicator is to 1, the higher the influence of the relevant factors on the security of information in the security system.

6. Discussion of the results of assessing the current state of a multi-contour information security system

The emergence of socio-cyberphysical systems (block diagram in Fig. 1) requires new approaches to building security systems. First, a new approach to building multi-contour systems is needed, taking into account platforms and safety loops. Secondly, it is necessary to take into account the possibility of differentiating information resources (Table 1) taking into account the technologies on which the cyberphysical one is built. Thirdly, the need to use post-quantum algorithms, among which crypto-code constructions “stand out”. Such post-quantum algorithms make it possible to build asymmetric cryptosystems that are resistant in the post-quantum cryptoperiod, and also to provide the required level of efficiency and increase the level of reliability in an integrated manner.

To ensure security in multi-contour information security systems, it is proposed to use, firstly, post-quantum algorithms, since the emergence of a full-scale computer may occur in the next year or two. At the same time, US NIST experts question the possibility of using symmetric and asymmetric cryptography cryptosystems, which will ensure the required level of security. The competition

for post-quantum algorithms showed the possibility of providing security services based on combining cryptography mechanisms with noise-resistant coding methods on lattices or Galois fields. However, it is necessary to use Galois fields (2^{10}–2^{13}), which is a significant drawback when using them in smart and Internet of Things technologies, which require low-capacity solutions and significant limitations on computational parameters. Thus, the need arose to "react" to this problem. Secondly, international regulators and legislation still consider the components of security and define threats and mechanisms of preventive action for each component. This approach does not allow for an objective assessment of the current state of the defense system, the possibility of synergy and hybridity of threats, or their integration with social engineering methods. To ensure the further development of post-quantum algorithms – crypto-code constructions, it is proposed to use a modification of noise-resistant codes (shortening and lengthening). This approach makes it possible to ensure the required level of security over the GF(2^6–2^8) without compromising security. Resilience is ensured using additional initialization vectors: when shortened, the initialization vector "indicates" the number and places of "removal" of symbols in the codogram (cryptogram). A further reduction in the computational and capacitive parameters of building a hybrid crypto-code design is defective codes. Analysis [1–3] showed that the use of HCCC provides a significant reduction in the complexity of generating (≈12 times) and decoding (≈20 times) a cryptogram compared to the McEliece crypto-code construction on classical codes. At the same time, HCCC can be built over the GF(2^4–2^6), which allows reducing computational and capacity costs, while resistance is ensured by transmitting damaged text and damage (the "reduction" rules in each plaintext character).

The analysis of the use of various noise-resistant codes in crypto-code constructions and the analysis of technologies for constructing socio-cyberphysical systems based on smart technologies (Tables 1, 2) showed that the use of various codes allows to differentiate the main indicators of cryptosystems and take into account the level of secrecy of information resources. This approach will reduce not only computational and capacity costs, but also increase the level of security through various modifications and selection of noise-resistant codes. This mechanism will reduce the possibility of hacking crypto-code constructions and provide the required level of security. Fig. 5, 6 present a methodology for constructing multi-contour information security systems, which ensures an objective assessment of the current state of security of infrastructure elements of socio-cyberphysical systems. The construction of a multi-contour protection system based on post-quantum algorithms will ensure the required level of security, taking into account the amount of secrecy of information resources, their circulation and storage.

A promising direction is the use of neural networks and "adding" threats from metric databases, for example KDD99 NCL, which will "expand" the range of threats and vulnerabilities, as well as provide the required level of objectivity for taking preventive measures.

7. Conclusions

1. The analysis of threats to socio-cyberphysical systems (critical infrastructure objects) allows to formulate a methodology for constructing multi-contour information protection systems. One of the main elements of such systems is proposed to use post-quantum algorithms – crypto-code constructions based on various noise-resistant codes with the possibility of causing damage. The proposed McEliece crypto-code constructions on LDPC codes ensure efficiency and durability, providing the required level of basic security services.

2. The proposed block diagram of the methodology for constructing multi-contour information security systems provides the opportunity to obtain an objective assessment of the current state of security in socio-cyberphysical systems. The proposed assessment software package allows to obtain an integrated security indicator, identify critical points of vulnerability and the "opportunity" of an attacker to gain access to confidential information. And the proposed mechanisms and protocols based on post-quantum algorithms will provide the required level of stability and efficiency during the period of the emergence of a full-scale quantum computer.

Conflict of interest

The authors declare that there are no conflicts of interest regarding this study, including financial, personal, authorship or other nature, which could affect the research and its results presented in this article.

Financing

The study was conducted without financial support.

Data availability

The manuscript has no associated data.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the presented work.

References

1. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S. et al.; Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.) (2021). Synergy of building cybersecurity systems. Kharkiv: PC TECHNOLOGY CENTER, 188. https://doi.org/10.15587/978-617-7319-31-2
2. Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M., Hrytsyk, V., Milov, O. et al.; Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M. (Eds.) (2022). Modeling of security systems for critical infrastructure facilities. Kharkiv: PC TECHNOLOGY CENTER, 196. https://doi.org/10.15587/978-617-7319-57-2

3. Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O., Korol, O., Milevskyi, S. et al.; Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O. (Eds.) (2023). Models of socio-cyber-physical systems security. Kharkiv: PC TECHNOLOGY CENTER, 184. https://doi.org/10.15587/978-617-7319-72-5
4. Yevseiev, S., Dzheniuk, N., Tolkachov, M., Milov, O., Voitko, T., Prygara, M. et al. (2023). Development of a multi-loop security system of information interactions in socio-cyberphysical systems. Eastern-European Journal of Enterprise Technologies, 5 (9 (125)), 53–74. https://doi.org/10.15587/1729-4061.2023.289467
5. Dzheniuk, N., Yevseiev, S., Lazurenko, B., Serkov, O., Kasilov, O. (2023). A method of protecting information in cyber-physical space. Advanced Information Systems, 7 (4), 80–85. https://doi.org/10.20998/2522-9052.2023.4.11
6. Shmatko, O., Herasymov, S., Lysetskyi, Y., Yevseiev, S., Sievierinov, O., Voitko, T. et al. (2023). Development of the automated decision-making system synthesis method in the management of information security channels. Eastern-European Journal of Enterprise Technologies, 6 (9 (126)), 39–49. https://doi.org/10.15587/1729-4061.2023.293511
7. Haag, S., Siponen, M., Liu, F. (2021). Protection Motivation Theory in Information Systems Security Research. ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 52 (2), 25–67. https://doi.org/10.1145/3462766.3462770
8. Li, Y., Xin, T., Siponen, M. (2022). Citizens' Cybersecurity Behavior: Some Major Challenges. IEEE Security & Privacy, 20 (1), 54–61. https://doi.org/10.1109/msec.2021.3117371
9. Shmatko, O., Balakireva, S., Vlasov, A., Zagorodna, N., Korol, O., Milov, O. et al. (2020). Development of methodological foundations for designing a classifier of threats to cyberphysical systems. Eastern-European Journal of Enterprise Technologies, 3 (9 (105)), 6–19. https://doi.org/10.15587/1729-4061.2020.205702
10. Khoroshko, V. O., Pavlov, I. M., Bobalo, Y. Ya., Dudykevich, V. B. et al. (2020). Design of complex information protection systems. Lviv: Ed. Lviv Polytechnic, 320.
11. Brailovskyi, M. M., Zybin, S. V., Piskun, I. V., Khoroshko, V. O., Khokhlacheva, Yu. E. (2021). Information protection technologies. Kyiv: Central Committee "Comprint", 296.
12. Dudykevich, V. B., Khoroshko, V. O., Yaremchuk, Yu. E. (2018). Basics of information security. Vinnytsia: Ed. He. national technical Univ, 315.
13. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. FIPS PUB 202. https://doi.org/10.6028/NIST.FIPS.202
14. Migration to Post-Quantum Cryptography. Available at: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms
15. Clarridge, A., Salomaa, K. (2009). A Cryptosystem Based on the Composition of Reversible Cellular Automata. Lecture Notes in Computer Science, 314–325. https://doi.org/10.1007/978-3-642-00982-2_27
16. Lightweight Cryptography. Available at: https://csrc.nist.gov/Projects/lightweight-cryptography
17. Davydiuk, A. (2023). Implementation of new tools and methods for increasing the level of cyber security of critical infrastructure objects. Ukrainian Scientific Journal of Information Security, 25 (3). https://doi.org/10.18372/2410-7840.25.17937
18. Khomik, M., Harasymchuk, O. (2023). Analysis of threats to generators of pseudo-random numbers and pseudo-random sequences and protection measures. Ukrainian Information Security Research Journal, 25 (4). https://doi.org/10.18372/2410-7840.25.18222
19. Klimovych, S. (2023). Methodology of traffic masking in a specialized data transmission network. Ukrainian Scientific Journal of Information Security, 25 (3). https://doi.org/10.18372/2410-7840.25.17935
20. Risk assessment methodologies. Available at: https://www.cisa.gov/sites/default/files/publications/Risk%2520Assessment%2520Methodologies.pdf
21. UNOCT launches Update of the UN Compendium of Good Practices on the Protection of Critical Infrastructure against Terrorist Attacks. Available at: https://www.un.org/counterterrorism/events/unoct-launches-2022-update-un-compendium-good-practices-protection-critical-infrastructure
22. Methodology for assessing regional infrastructure resilience (2021). Washington. Available at: https://www.cisa.gov/sites/default/files/publications/DIS_DHS_Methodology_Report_ISD%2520EAD%2520Signed_with%2520alt-text_0.pdf
23. Theocharidou, M., Giannopoulos, G. (2015). Risk assessment methodologies for critical infrastructure protection. Part II, A new approach. Publications Office of the European Union. https://doi.org/10.2788/621843
24. Giannopoulos, G., Dorneanu, B., Jonkeren, O. (2013). Risk Assessment Methodology for Critical Infrastructure Protection. EUR 25745 EN. Luxembourg (Luxembourg): Publications Office of the European Union. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC78292
25. Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide (2018). Available at: https://www.fema.gov/sites/default/files/2020-07/threat-hazard-identification-risk-assessment-stakeholder-preparedness-review-guide.pdf
26. National Protection Framework (2016). Available at: https://www.fema.gov/sites/default/files/2020-04/National_Protection_Framework2nd-june2016.pdf

27. Yevseiev, S., Hryhorii, K., Liekariev, Y. (2016). Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system. Eastern-European Journal of Enterprise Technologies, 6 (4 (84)), 11–23. https://doi.org/10.15587/1729-4061.2016.86175
28. Yevseiev, S., Korol, O., Kots, H. (2017). Construction of hybrid security systems based on the crypto-code structures and flawed codes. Eastern-European Journal of Enterprise Technologies, 4 (9 (88)), 4–21. https://doi.org/10.15587/1729-4061.2017.108461
29. Yevseiev, S., Tsyhanenko, O., Ivanchenko, S., Aleksiyev, V., Verheles, D., Volkov, S. et al. (2018). Practical implementation of the Niederreiter modified cryptocode system on truncated elliptic codes. Eastern-European Journal of Enterprise Technologies, 6 (4 (96)), 24–31. https://doi.org/10.15587/1729-4061.2018.150903
30. Yevseiev, S., Tsyhanenko, O., Gavrilova, A., Guzhva, V., Milov, O., Moskalenko, V. et al. (2019). Development of Niederreiter hybrid crypto-code structure on flawed codes. Eastern-European Journal of Enterprise Technologies, 1 (9 (97)), 27–38. https://doi.org/10.15587/1729-4061.2019.156620
31. Yevseiev, S., Havrylova, A., Korol, O., Dmitriiev, O., Nesmiian, O., Yufa, Y., Hrebennikov, A. (2022). Research of collision properties of the modified UMAC algorithm on crypto-code constructions. EUREKA: Physics and Engineering, 1, 34–43. https://doi.org/10.21303/2461-4262.2022.002213
32. Yevseiev, S., Havrylova, A., Milevskyi, S., Sinitsyn, I., Chalapko, V., Dukin, H. et al. (2023). Development of an improved SSL/TLS protocol using post-quantum algorithms. Eastern-European Journal of Enterprise Technologies, 3 (9 (123)), 33–48. https://doi.org/10.15587/1729-4061.2023.281795
33. Pohasii, S., Yevseiev, S., Zhuchenko, O., Milov, O., Lysechko, V., Kovalenko, O. et al. (2022). Development of crypto-code constructs based on LDPC codes. Eastern-European Journal of Enterprise Technologies, 2 (9 (116)), 44–59. https://doi.org/10.15587/1729-4061.2022.254545
34. Yevseiev, S., Abdalla, A., Osiievskyi, S., Larin, V., Lytvynenko, M. (2020). Development of an advanced method of video information resource compression in navigation and traffic control systems. EUREKA: Physics and Engineering, 5, 31–42. https://doi.org/10.21303/2461-4262.2020.001405
35. Korchenko, A., Breslavskyi, V., Yevseiev, S., Zhumangalieva, N., Zvarych, A., Kazmirchuk, S. et al. (2021). Development of a method for constructing linguistic standards for multi-criteria assessment of honeypot efficiency. Eastern-European Journal of Enterprise Technologies, 1 (2 (109)), 14–23. https://doi.org/10.15587/1729-4061.2021.225346
36. Yevseiev, S., Kuznietsov, O., Herasimov, S., Horielyshev, S., Karlov, A., Kovalov, I. et al. (2021). Development of an optimization method for measuring the Doppler frequency of a packet taking into account the fluctuations of the initial phases of its radio pulses. Eastern-European Journal of Enterprise Technologies, 2 (9 (110)), 6–15. https://doi.org/10.15587/1729-4061.2021.229221
37. Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A., Mykus, S. et al. (2021). Development of a concept for building a critical infrastructure facilities security system. Eastern-European Journal of Enterprise Technologies, 3 (9 (111)), 63–83. https://doi.org/10.15587/1729-4061.2021.233533
38. Yevseiev, S., Laptiev, O., Lazarenko, S., Korchenko, A., Manzhul, I. (2021). Modeling the protection of personal data from trust and the amount of information on social networks. EUREKA: Physics and Engineering, 1, 24–31. https://doi.org/10.21303/2461-4262.2021.001615
39. Cybersecurity classifier. Available at: https://skl.sspu.sumy.ua/
40. Milevsky, S. (2023). Development of threat classifier in socio-cyber-physical systems. Ukrainian Scientific Journal of Information Security, 29 (3). https://doi.org/10.18372/2225-5036.29.18070
41. Yevseiev, S., Milevskyi, S., Bortnik, L., Voropay, A., Bondarenko, K., Pohasii, S. (2022). Socio-Cyber-Physical Systems Security Concept. 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). https://doi.org/10.1109/hora55278.2022.9799957
42. Yevseiev, S., Ryabukha, Y., Milov, O., Milevskyi, S., Pohasii, S., Melenti, Y. et al. (2021). Development of a method for assessing forecast of social impact in regional communities. Eastern-European Journal of Enterprise Technologies, 6 (2 (114)), 30–43. https://doi.org/10.15587/1729-4061.2021.249313
43. Yevseiev, S., Pohasii, S., Milevskyi, S., Milov, O., Melenti, Y., Grod, I. et al. (2021). Development of a method for assessing the security of cyber-physical systems based on the Lotka–Volterra model. Eastern-European Journal of Enterprise Technologies, 5 (9 (113)), 30–47. https://doi.org/10.15587/1729-4061.2021.241638
44. Ranjitha, C. R., Thomas, J., Chithra, K. R. (2016). A brief study on LDPC codes. International Journal of Engineering Research and General Science, 4, (2), 612–618. Available at: http://pnrsolution.org/Datacenter/Vol4/Issue2/85.pdf
45. Broul′ım, J. (2018). LDPC codes - new methodologies. University of West Bohemia, 127. Available at: https://cds.cern.ch/record/2730008/files/CERN-THESIS-2018-479.pdf
46. Zhu, H., Pu, L., Xu, H., Zhang, B. (2018). Construction of Quasi-Cyclic LDPC Codes Based on Fundamental Theorem of Arithmetic. Wireless Communications and Mobile Computing, 2018, 1–9. https://doi.org/10.1155/2018/5264724
47. Singh, H. (2020). Code based Cryptography: Classic McEliece. arXiv.org. https://doi.org/10.48550/arXiv.1907.12754

48. Otmani, A., Tillich, J.-P., Dallot, L. (2010). Cryptanalysis of Two McEliece Cryptosystems Based on Quasi-Cyclic Codes. Mathematics in Computer Science, 3 (2), 129–140. https://doi.org/10.1007/s11786-009-0015-8
49. Liva, G., Song, S., Lan, L., Zhang, Y., Lin, S., Ryan, W. E. (2017). Design of LDPC Codes: A Survey and New Results. Journal of Communications Software and Systems, 2 (3), 191. https://doi.org/10.24138/jcomss.v2i3.283
50. Richardson, T. J., Urbanke, R. L. (2001). Efficient encoding of low-density parity-check codes. IEEE Transactions on Information Theory, 47 (2), 638–656. https://doi.org/10.1109/18.910579
51. Chandrasetty, V. A., Aziz, S. M. (2011). FPGA Implementation of a LDPC Decoder using a Reduced Complexity Message Passing Algorithm. Journal of Networks, 6 (1). https://doi.org/10.4304/jnw.6.1.36-45
52. Wang, Y. (2008). Generalized constructions, decoding and implementation of LDPC codes. University of Hawaii at Manoa.
53. Rukhin, A., Sota, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S. et al. (2000). A statistical test suite for random and pseudorandom number generators for cryptographic applications. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-22
54. Milevsky, S. (2023). Sociocyberphysical systems' security models. Ukrainian Information Security Research Journal, 25 (4). https://doi.org/10.18372/2410-7840.25.18224