UDC 004.056.5:355.58 **doi:** https://doi.org/10.20998/3083-6298.2025.03.07

Yevhen Melenti[1], Pierre Murr[2], Iryna Aksonova[3], Illia Bukatych[3], Oleksandr Sitchenko[3]

[1] National Academy of Security Service of Ukraine, Kyiv, Ukraine
[2] International University of Science and Technology in Kuwait, Ardiya Government Area, Kuwait
[3] National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

INTEGRATED ASSESSMENT OF THE CYBERSECURITY LEVEL OF CRITICAL INFRASTRUCTURE IN A POST-QUANTUM ENVIRONMENT

Abstract. The relevance of the study is due to the increasing complexity of cyber threats in the post-quantum environment, the development of quantum computing technologies and the intellectualization of data management and processing processes. In the context of the spread of hybrid and synergistic attacks combined with social engineering methods, traditional approaches to assessing the security of critical infrastructure objects (CIF) are becoming ineffective. This requires the implementation of an integrated methodology for assessing the level of cyber security, capable of adaptively reflecting the real state of security and taking into account the impact of post-quantum threats. **The subject of the study** is the process of integrated assessment of the level of cyber security of CIF in the post-quantum environment using mathematical and analytical methods. **The purpose of the article** is to develop a methodology for integrated assessment of the level of security of CIF in the post-quantum environment taking into account modern hybrid and synergistic cyber threats. **Results obtained**. A methodology for assessing the level of security based on a synergistic threat model is proposed, which takes into account the categories of attackers, their goals, resources and capabilities. A mathematical formalization of a unified classifier of cyber threats has been developed, which forms tuples taking into account the features of hybridity, synergy, and social engineering factors. A mathematical apparatus has been formed for modeling the implementation of cyber threats and determining the level of resilience of CIF cyber systems in a post-quantum environment. **Conclusions.** Assessment of CIF security makes it possible to identify critically important information assets, assess the effectiveness of protection measures, and identify vulnerable elements. The results of the study confirm the feasibility of implementing intelligent multi-circuit protection systems based on post-quantum algorithms to ensure the appropriate level of cyber resilience in a post-quantum environment.

Keywords: post-quantum threats, synergistic cyber threat model, integrated safety indicator, critical infrastructure facility, intelligent multi-circuit protection system.

Introduction

Problem relevance. Ensuring the cyber security of critical infrastructure facilities (CIF) is one of the key factors of national security, especially in the context of the rapid development of post-quantum technologies and intelligent information systems. Revolutionary changes in the electronics industry, the integration of infocommunication and computer networks into a single cyberspace, as well as the spread of smart technologies have contributed to the formation of socio-cyberphysical systems (SCPS), which has significantly increased the level of complexity of threats to critical facilities.

Critical infrastructure, which is the basis of society's life, is becoming increasingly vulnerable due to the openness of standards, integration with web technologies and connection to global networks. Cyberattacks on control systems (in particular SCADA) can lead to disruption of the functioning of transport, energy, financial and municipal services, as well as create real risks in the physical space. Compounding the problem is that a significant portion of attacks go unnoticed or unreported for business security reasons.

In today's environment, the struggle between cybercriminals and defenders remains asymmetric: a minimal resource is enough for a successful attack, while effective protection requires comprehensive and multi-level solutions. This necessitates the creation of new methodological foundations for building integrated, intelligent, and multi-circuit cyber defense systems capable of ensuring the resilience of critical infrastructure to post-quantum threats and dynamic changes in cyberspace.

Literature review. Literature analysis shows that critical infrastructure control systems, in particular supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and programmable logic controllers (PLC), are traditionally considered to be among the most attractive targets for cyberattacks. Thus, in [1], modern threats to ICS/OT systems and their vulnerabilities due to the integration of IT/OT networks were analyzed. In [2], the implementation of artificial intelligence and machine learning for detecting attacks in SCADA and IoT/IIoT environments is considered. The authors of [3] consider challenges and solutions in the field of post-quantum cryptography (PQC) for protecting critical infrastructure. The study [4] provides a methodology for assessing cyber risks for automation systems used in OKI. Also, in [5], the global and national challenges posed by the emergence of quantum computing for information security are considered.

Despite the large volume of scientific works, the analysis shows that there is no single concept and comprehensive methodology for building an integrated system for protecting CIF, taking into account new hybrid and synergistic threats in the post-quantum environment. A significant part of the publications focuses on individual aspects (SCADA, IIoT, PQC), but does not comprehensively cover the process of integrated

assessment of the level of cyber security, taking into account human, computational and economic factors, which emphasizes the relevance of the topic of this article.

Therefore, taking into account the above, the purpose of this article is to develop a methodology for integrated assessment of the level of security of CIF in the post-quantum environment, taking into account modern hybrid and synergistic cyber threats.

1. Assessment of target threats based on a unified classifier

It is proposed to assess the target threats to automated data transmission systems of the CIF with signs of hybridity and synergy, as well as their possibility of integration with social engineering methods, based on the classification of threats by a unified classifier based on the proposed framework [6-7]. Fig. 1 shows the mathematical formalization of the unified classifier, which allows forming tuples-classifiers of cyber threats taking into account not only the signs of their hybridity and synergy, integration with social engineering methods, as well as their orientation to one or another platform of socio-cyber-physical systems.

$$C^{i}_{\substack{\text{threat}\\\text{vector}}} = \left\{ L^{1}_{\substack{\text{criticality}\\\text{of the threat}}}, L^{2}_{\substack{\text{security}\\\text{component}}}, L^{3}_{\substack{\text{security}\\\text{service}}}, L^{4}_{\substack{\text{the nature of}\\\text{the threat's direction}}}, L^{5}_{\substack{\text{threat impact}\\\text{level}}}, L^{6}_{\substack{\text{social impact}\\\text{engineering}}}, L^{7}_{\substack{\text{platform}\\\text{contour}}} \right\},$$

$$L^{1}_{\substack{\text{criticality}\\\text{of the threat}}} \in \left\{ \begin{array}{l} 01 - \text{critical, } 02 - \text{high, } 03 - \text{medium,} \\ 04 - \text{low, } 05 - \text{very low} \end{array} \right\};$$

$$L^{2}_{\substack{\text{security}\\\text{component}}} \in \left\{ \begin{array}{l} 01 - \text{cybersecurity, } 02 - \text{information security,} \\ 03 - \text{security of information} \end{array} \right\};$$

$$L^{3}_{\substack{\text{security}\\\text{service}}} \in \left\{ \begin{array}{l} 01 - \text{integrity, } 02 - \text{confidentiality, } 03 - \text{accessibility,} \\ 04 - \text{authenticity, } 05 - \text{undeniability} \end{array} \right\};$$

$$L^{4}_{\substack{\text{the nature of}\\\text{the threat's direction}}} \in \left\{ \begin{array}{l} 01 - \text{engineering and technical, } 02 - \text{organizational,} \\ 03 - \text{regulatory} \end{array} \right\};$$

$$L^{5}_{\substack{\text{threat impact}\\\text{level}}} \in \left\{ \begin{array}{l} 01 - \text{physical level, } 02 - \text{network layer,} \\ 03 - \text{operating system level, } 04 - \text{database management system level,} \\ 05 - \text{application and service level, } 06 - \text{IoT level,} \\ 07 - \text{level of information protection systems} \end{array} \right\};$$

$$L^{6}_{\substack{\text{social impact}\\\text{engineering}}} \in \left\{ \begin{array}{l} 01 - \text{system hack, } 02 - \text{system compromise,} \\ 03 - \text{data compromise,} \\ 04 - \text{finding critical points of the system,} \\ 05 - \text{information gathering} \end{array} \right\};$$

$$L^{7}_{\substack{\text{platform}\\\text{contour}}} \in \left\{ \begin{array}{l} 01 - \text{internal, } 02 - \text{external,} \\ 03 - \text{internal and external} \end{array} \right\}.$$

Fig. 1. Mathematical formalization of the unified classifier

In addition, the infrastructure of socio-cyber-physical systems is proposed to be divided into three platforms: a physical systems platform, a management platform (usually located in the cloud) and a social network platform. In this case, the hybridity of targeted (mixed) attacks refers to the impact of an attack on one of the security services (I, C, Ac, Aut, Un) on all security components (cybersecurity, information security, information security). The synergy of targeted (mixed) attacks refers to the impact of an attack on one security component (cybersecurity, information security, information security), but on all services simultaneously (I, C, Ac, Aut, Un). The formation of complex (multi-level) protection of a critical infrastructure object is formed on the basis of a hierarchical structure of the synthesis of information protection systems of cyber-physical systems, Internet technologies and computer networks, as well as mobile technologies. This approach makes it possible to form a synergistic model of threats to critical infrastructure facilities, taking into account the impact of cyberterrorists on its elements (Fig. 2).

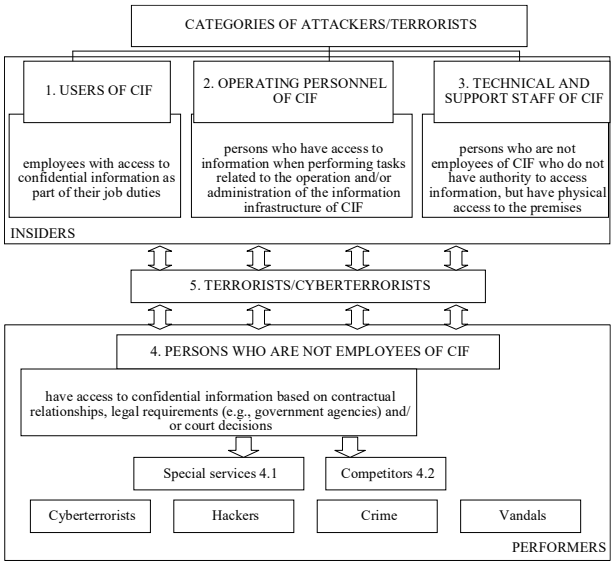

Fig. 2. Classification of attackers

Fig. 2 presents a classification of categories of attackers and terrorists that can affect critical infrastructure facilities (CIF). Fig. 2 demonstrates that threats can come from both the internal environment - from users, operational or technical personnel (insiders), and from the outside, from cyberterrorists or individuals not directly related to CIF. This structure emphasizes the need for a comprehensive approach to cyber defense, which should take into account both internal and external sources of risk, as well as the specific motivations of each category of potential attackers.

2. Formation of a model for implementing cyber threats and protecting cyber systems of CIF

To form a model of the implementation of a terrorist act and the degree of protection of cyber systems of a critical infrastructure facility, the following mathematical apparatus was developed:

classification allowed to introduce elements of many categories of attackers $L_i^{del} \in \left\{ L^{del} \right\} : L_1^{del}$ – users of CIF; L_2^{del} – operating personnel of CIF; L_3^{del} – technical support staff of CIF; L_4^{del} – persons who are not employees of CIF; L_5^{del} – terrorists and perpetrators of terrorist acts: L_{51}^{del} – cyberterrorists, L_{41}^{del} – special

services, L_{52}^{del} – hackers, L_{42}^{del} – competitors, L_{53}^{del} – criminals, L_{54}^{del} – vandals;

the model for carrying out a terrorist act is defined as:

$G_{\text{terror}}^{CFS\ CIF} = \left\{ L_i^{del}, \beta_i^{CPS\ CIF} \in \left\{ \beta_{\text{terror}}^{CPS\ CIF} \right\}, p_{rj}, r_{\text{motiv}}, T \right\}$,

where $L_i^{del} \in \left\{ L_i^{del} \right\}$ – terrorist criminal identifier; $\beta_i^{CPS\ CIF} \in \left\{ \beta_{terror}^{CPS\ CIF} \right\}$ – the weighting factor of the capabilities of a terrorist who committed a terrorist act against a CIF; prj – probability of at least one threat to the j-th asset, i – threat, n – $\forall i \in n$, number of threats; j – information resource (asset); $\forall j \in m$, m – number of assets; rmotiv – stimulation of a terrorist criminal to commit a terrorist act based on the indicators of a CIF; T – time of successful implementation of the threat. Analysis of attacker categories allows you to form an expert assessment and obtain a weighting factor for the possibility of threats (i-th threat);

the weighting factor of the terrorist perpetrator's capabilities is defined as [8]:

$\gamma_{terror}^{CPS\ CIF} = \frac{1}{N} \sum_{i=1}^{N} \beta_i^{CPS\ CIF} \times p_{rj} \times r_{motiv}$, where

$\beta_i^{CIF} = W_{cp}^{CIF} \cap W_{cash}^{CIF} \cap T$ – the weight of the capabilities of a terrorist criminal; $W_{cp}^{CPS\ CIF}$ – computing resources of a terrorist criminal; $W_{cash}^{CPS\ CIF}$ – financial resources of the terrorist perpetrator.

The proposed approach makes it possible to unify the procedure for determining the probability of a terrorist act on CIF, taking into account the capabilities of the terrorist perpetrator, both financial and computational resources.

Analysis of the infrastructure level of CIF and categories of terrorist perpetrators allows us to form a set {Hj}, which forms the levels of influence on the critical management object: technical channel level (H0); ISO/OSI physical level (H1); ISO/OSI channel level (H2); ISO/OSI network level (H3); ISO/OSI transport level (H4); ISO/OSI application level (H5); level of physical protection of CIF elements (video surveillance, sensors, grilles, locks, etc.) (H6); level of possible built-in devices (ventilation ducts, power lines, etc.) (H7);

the matrix of the relationship between the category of terrorist perpetrator and the level of influence on the OKI is defined as (Fig. 3).

Thus, the matrix of interaction between terrorist categories and levels of influence on the information-structural component makes it possible to determine the category of terrorist-perpetrator using the proposed method using the threat classifier by stages:

$$M_{L_i^{del}}^{H_i} = \left\| L_i^{del} \right\| \times \left\| H_i \right\| = \begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{matrix}.$$

Fig. 3. Matrix of the relationship between the category of terrorist offender and the level of influence on CIF

Stage 1. Determining the level of impact on the CIF from the set {H};

Stage 2. Determining the threat according to the CIF threat classifier;

Stage 3. Determining the relationship matrix between the category of terrorist-criminal and the level of impact on the CIF;

Stage 4. Identifying a possible terrorist from the relationship matrix;

Stage 5. Forming the concept of building a multi-circuit intellectual system of anti-terrorist protection of the CIF.

3. Construction of a multi-circuit intelligent anti-terrorist protection system CIF

Given the literature review and the identified unresolved issues in ensuring comprehensive protection of CIF, especially in the context of hybrid and post-quantum threats, it is advisable to move to the development of a multi-circuit intelligent system of anti-terrorist protection of CIF. Such a system should provide dynamic monitoring of the security situation, adaptive response to changing nature of attacks, as well as synergistic interaction between technical, analytical and organizational circuits of cyber defense.

Fig. 4 shows a structural diagram of the construction of a multi-circuit intelligent anti-terrorist protection system of the CIF.

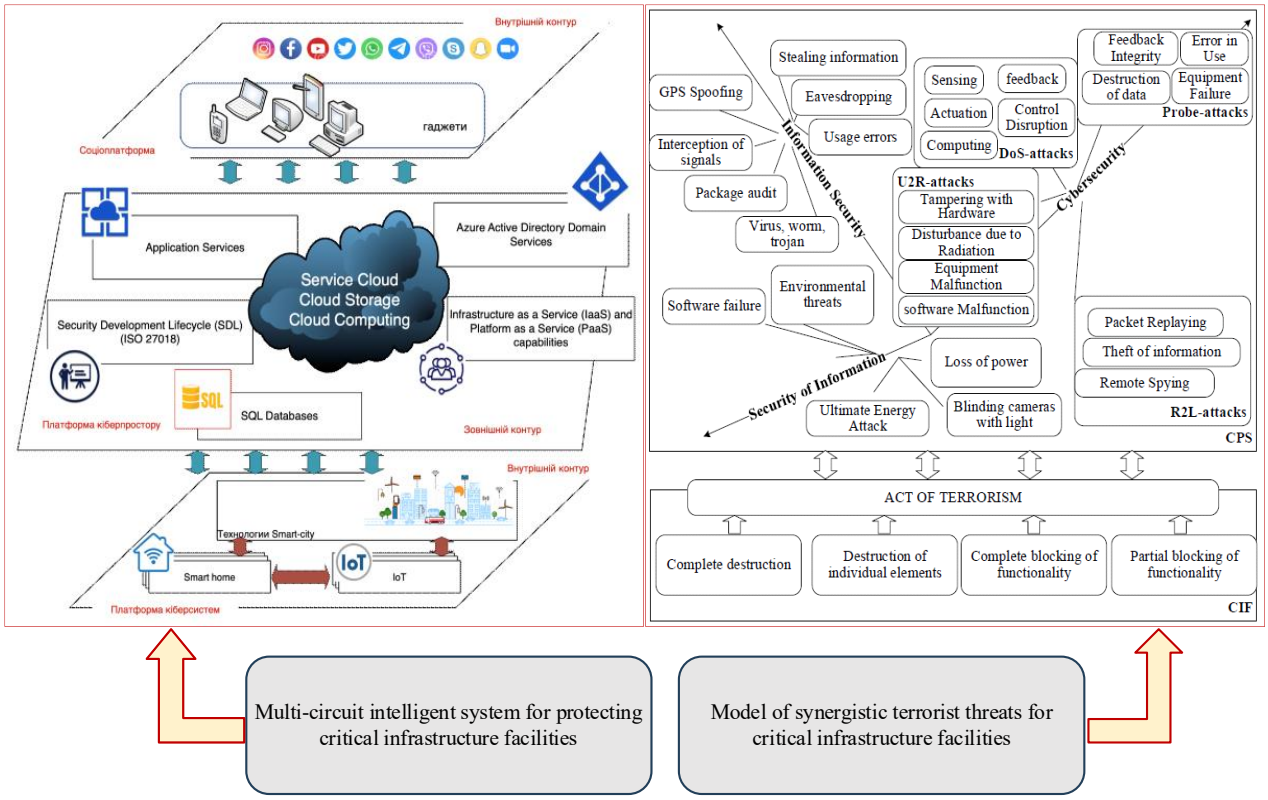

Fig. 4. Structural diagram of the construction of a multi-circuit intelligent anti-terrorist protection system CIF

Fig. 4 demonstrates the relationship between a multi-circuit intelligent system for protecting critical infrastructure objects and a model of synergistic terrorist threats that are formed in modern cyberspace. The presented system implements a combination of cloud services, IoT components, security services and analytical platforms, providing a comprehensive approach to monitoring, detecting and neutralizing attacks of various nature. On the other hand, the threat model illustrates how cyberattacks, physical influences and socio-technical factors can combine to create the effect of synergistic terror against elements of the CIF.

Thus, the interaction between these two aspects allows us to build a holistic concept of cyber defense, capable of responding to complex multi-level threats in real time. To ensure the effectiveness of such a system, it is necessary to develop a methodology for assessing the streaming state of the CIF security level, which will allow us to quantitatively determine the current level of security, promptly detect deviations and adapt protective circuits in accordance with the dynamics of threats.

4. Construction of a methodology for assessing the state of the security level of the CIF

As the analysis showed, to ensure effective management of cyber defense of CIF, it is necessary to have a formalized tool that allows not only to detect threats, but also to assess the current state of the security level in real time. Such an approach provides the ability to adaptively respond to changes in the cyber threat environment and increases the resistance of CIF to multi-layered attacks.

In this context, a methodology for assessing the flow state of the CIF security level is proposed, which is based on the integration of data from various protection mechanisms, taking into account the dynamics of incidents and the application of intelligent information processing algorithms. The following material is devoted to the stages of formation and implementation of this methodology - from the definition of key security indicators to the construction of an integrated cyber resilience index.

The main stages of the methodology are presented in Fig. 5.

As can be seen from Fig. 5, the stages of the methodology for assessing the flow state of the security level of critical infrastructure facilities are based on a combination of quantitative and qualitative indicators, as well as the use of a matrix approach to describing the relationships between information resources, threats, and the level of security.

Below is a brief description of each stage.

At the first stage, the current cyber threats for critical infrastructure facilities are identified and described, taking into account their specifics, architecture and operating environment. Experts determine the key parameters of each threat, such as source, type, intensity, potential impact and probability of implementation. Based on these characteristics, a set of cyber threats is formed, which serves as the basic structural unit for further analysis and construction of security risk matrices.

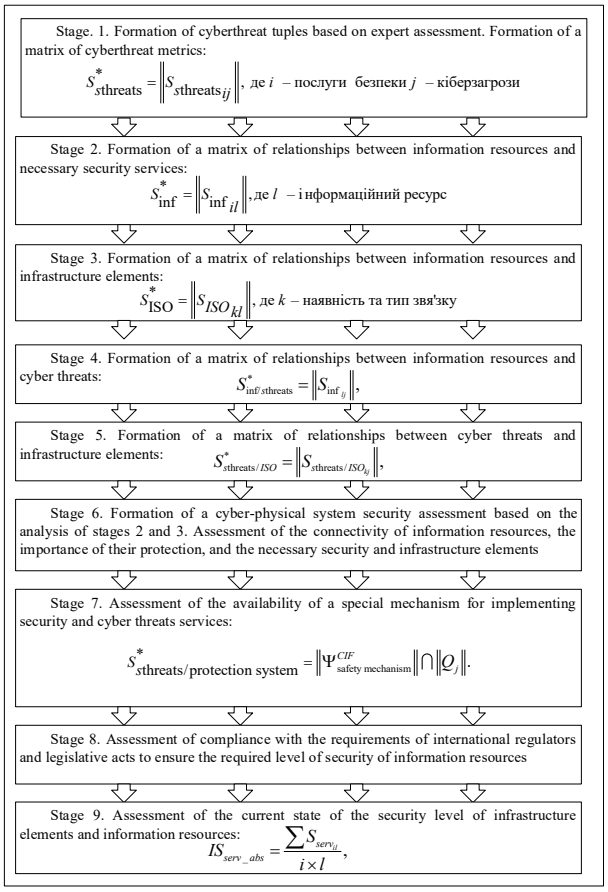

Fig. 5. Stages of the methodology for assessing the flow state of the CIF security level

The second stage involves assessing the criticality of each information resource to ensure the stability of the CIF. Priorities are determined by level of importance, which allows you to focus on the most significant elements of the system.

The third stage assesses how vulnerability or damage to one resource can affect other elements of the system. This step provides an understanding of the cascading effect within the infrastructure.

The fourth stage creates a structural model of dependencies between physical, logical and cyber elements of the infrastructure. This allows you to reflect how a failure in one element can lead to a disruption in the functioning of other components.

The fifth stage determines the attack vectors through which specific cyber threats can be implemented on individual elements of the CIF. The resulting matrix helps to build an attack model and predict potential penetration paths.

At the sixth stage, based on the previous matrices, an integrated model is formed that combines the relationships between threats, resources, and infrastructure elements. It allows calculating the current level of risk and the degree of stability of the system in dynamics.

At the seventh stage, the capabilities of special mechanisms for ensuring the security of automated data transmission systems and socio-cyber-physical systems are assessed.

The following steps are proposed for the implementation of this stage:

Step 1. Assessment of possible APT attacks on infrastructure elements, defined as: $S^*_{\text{malefactors/ ISO}} = \left\| S_{ISO\ pl} \right\|$, where p – type of attacker.

Step 2. Assess the attackers' capabilities (financial, computational, human). The attacker's "danger" weight is defined as:

$$p^{CIF}_{\text{malefactors}} = \frac{1}{N} \sum_{i=1}^{N} \beta^{CIF}_{p\ i},$$ where:

$\beta^{CIF}_i = Q^{CIF}_{\substack{\text{computing} \\ \text{resources}}} \cap Q^{SIF}_{\substack{\text{financial} \\ \text{resources}}} \cap Q^{SIF}_{\substack{\text{human} \\ \text{resources}}}$ – offender opportunity coefficient, $Q^{CIF}_{\substack{\text{computing} \\ \text{resources}}}, Q^{CIF}_{\substack{\text{financial} \\ \text{resources}}}, Q^{CIF}_{\substack{\text{human} \\ \text{resources}}} \in$ {1 – unlimited resources of cyberterrorists, 0,75 – state resources (special services), 0,5 – cybercriminal resources, 0,25 – resources of crime, competitors, hackers, 0,001 – vandal resources}.

Step 3. Assess the probability of implementing targeted (APT) attacks taking into account the attacker's "danger" coefficient, defined as: $\left\| Q_j \right\| = p^{CIF}_{\text{malefactors}_j} \times P^j_\alpha$, де j – threat; a – probability of cyber threat; $P^j_\alpha \in$ {1 – the threat is realized daily, 0,75 – the threat is realized within a week, 0,5 – the threat is realized within a month, 0,25 – the threat is realized within a year, 0,001 – unlimited time}.

Step 4. Assessment of the availability of special mechanisms for providing security services, we will determine according to Table 1 [9-12] by the formula:

$$\Psi^{CIF}_{\text{safety mechanism}} = \left\| F_{ij} \right\| \times \Psi_i, \quad (1)$$

where i – a special security (authentication) mechanism; j – a threat.

Step 5. Evaluation of preventive measures to counter ART attacks, defined as: $S^*_{\text{sthreats/protection system}} = \left\| \Psi^{CIF}_{\text{safety mechanism}} \right\| \cap \left\| Q_j \right\|$.

Table 1 – **Weighting coefficients Ψ and the presence of special mechanisms for ensuring security services and reliability of the data transmission system**

Mechanism type	Special mechanisms that ensure:															
	detection					alarm system					locking					
	level of stability					level of stability					level of stability					
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	
IDS	+	+	+	+	+	+	+	+	+	+	–	–	–	–	–	
IPS	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
SIEM	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
Mechanism type (bit)	Mechanisms that provide the service:															
	confidentiality					integrity					authenticity					certainty				
	level of stability					level of stability					level of stability					level of stability				
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Symmetric Block Ciphers (SBC)																				
SBC with key 128	+	–	–	–	–	+	–	–	–	–	+	–	–	–	–	–	–	–	–	–
MAC+SBC with key 256	+	+	–	–	–	+	+	–	–	–	+	+	–	–	–	–	–	–	–	–
SBC with key 256	+	+	+	–	–	+	+	+	–	–	+	+	+	–	–	–	–	–	–	–
MAC+SBC with key 256	+	+	+	+	–	+	+	+	+	–	+	+	+	+	–	–	–	–	–	–
SBC with key 256	+	+	+	+	+	+	+	+	+	+	+	+	+	+	–	–	–	–	–	–
Symmetric Stream Ciphers (SSC)																				
Uniform movement of registers	+	+	+	–	–	+	+	+	–	–	+	+	+	–	–	+	+	+	–	–
Uneven movement of registers	+	+	+	+	–	+	+	+	+	–	+	+	+	+	–	+	+	+	+	–
Asymmetric algorithms																				
Digital signature (DS)	+	+	+	–	–	+	+	+	–	–	+	+	+	–	–	–	–	–	–	–
On EC	+	+	+	+	–	+	+	+	+	–	+	+	+	+	–	–	–	–	–	–
Post-quantum algorithms																				
DS	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	–	–	–	–	–
HCCD on MEC	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
CCC on MEC (EC)	+	+	+	+	–	+	+	+	+	–	+	+	+	+	+	+	+	+	+	+
CCC on LDPC	+	+	+	–	–	+	+	+	–	–	+	+	+	–	–	+	+	+	+	+

Примітка: $\Psi_i \in$ {1 рівень – 0,1, 2 рівень – 0,25, 3 рівень – 0,5, 4 рівень – 0,75, 5 рівень – 1}, SBC – block symmetric cipher, SSC – stream symmetric cipher, MAC – message authentication code, DS – digital signature, EC – asymmetric algorithms on elliptic curves, HCCD – hybrid crypto-code designs, CCC – crypto code constructions (McEliece, Niederreite), CCC на MEC (EC) – CCC on modified (shortened, extended) elliptical codes (EC).

At the eighth stage, the compliance of the CIF cyber security system with regulatory requirements, international standards and industry recommendations is checked. The degree of implementation of security policies, risk management procedures, incident response and access control is assessed. The result is the determination of the level of regulatory compliance and the identification of gaps between the actual and target state of cyber security, which allows for the formation of recommendations for increasing the level of compliance and security.

At the ninth stage, a final integrated indicator of the level of cyber security is formed, which reflects the current state of security of the facility in real time. The indicator can be used for monitoring, forecasting incidents and making management decisions to increase the cyber resilience of the system.

5. Mathematical apparatus for forming integral indicators of the level of security and level of protection of the CIF

After calculating the key relationship matrices, the synergistic effect of the interaction of cybersecurity components (security services, information resources, infrastructure elements) is determined.

I. 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 (S_{inf_i}) and system resource (S_{inf_l}), де i=1,...,5, l=1,...,8, by the formulas:

$$S_{\text{inf}_i} = \sum_{l=1}^{8} S_{\text{inf}_{il}}\,,\; S_{\text{inf}_l} = \sum_{i=1}^{5} S_{\text{inf}_{il}}\,. \qquad (2)$$

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

$$S_{\text{inf}_i s} = \sum_{i=1}^{5} S_{\text{inf}_i}\,,\; S_{\text{inf}_l s} = \sum_{l=1}^{8} S_{\text{inf}_l}\,. \qquad (3)$$

Below are the weighting factors for services (αS_{inf_i}) and resources (αS_{inf_l}): $\alpha S_{\text{inf}_i} = \dfrac{S_{\text{inf}_i}}{S_{\text{inf}_i s}}$,

where I=1,...,5; $\alpha S_{\text{inf}_l} = \dfrac{S_{\text{inf}_l}}{S_{\text{inf}_l s}}$, where l=1,...,8.

Then, the services and resources are ranked according to specific weights from highest to lowest to determine the most significant services/resources according to the matrix of how they interact.

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

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

$$IS_{\text{inf}\_rel} = \frac{IS_{\text{inf}\_abs} - S_{\text{inf}_{il}}\min}{S_{\text{inf}_{il}}\max - S_{\text{inf}_{il}}\min}, \qquad (4)$$

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

II. For a matrix of dependencies between information resources and infrastructure layers (ISO/OSI models) where information circulates and/or is stored: $S^{*}_{\text{ISO}} = \left\| S_{ISO_{kl}} \right\|$, where k – availability and type of connection, element (level) of infrastructure where information is stored, l – information resource.

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

$$S_{ISO_k} = \sum_{l=1}^{7} S_{ISO_{kl}}\,,\; S_{ISO_l} = \sum_{k=1}^{8} S_{ISO_{kl}}\,. \qquad (5)$$

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

$$S_{ISO_k s} = \sum_{k=1}^{8} S_{ISO_k}\,,\; S_{ISO_l s} = \sum_{l=1}^{7} S_{ISO_l} \qquad (6)$$

Below are the weighting factors for resources (αS_{ISO_k}) and infrastructure layers (αS_{ISO_l}) by the formulas:

$$\alpha S_{ISO_k} = \frac{S_{ISO_k}}{S_{ISO_k s}}\,, \qquad (7)$$

where k=1,...,8;

$$\alpha S_{ISO_l} = \frac{S_{ISO_l}}{S_{ISO_l s}}, \qquad (8)$$

where l=1,...,7.

The resources and infrastructure levels are then ranked by specific weights from highest to lowest to determine the most significant resources/levels according to the matrix of how they interact.

Next, an *integral indicator of the current level of security* is formed for the correspondence matrix between information resources and infrastructure levels.

For this purpose, the absolute and relative values of the integral indicator are determined:

$$IS_{ISO\_abs} = \frac{\sum S_{ISO_{kl}}}{k \times l},$$

$$IS_{ISO\_rel} = \frac{IS_{ISO\_abs} - S_{ISO_{kl}}\min}{S_{ISO_{kl}}\max - S_{ISO_{kl}}\min}, \quad (9)$$

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 correspondence matrix between information resources and infrastructure levels; k - number of information resources; l - number of infrastructure levels; $S_{ISO_{kl}}\min$ – minimal element of the correspondence matrix between information resources and infrastructure levels; $S_{ISO_{kl}}\max$ – maximum element of the correspondence matrix between information resources and infrastructure levels.

III. For a correspondence 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 (S_{serv_i}) and each level of infrastructure (S_{serv_l}), where i=1,..,5, l=1,..,7, by the formulas:

$$S_{serv_i} = \sum_{l=1}^{7} S_{serv_{il}}, \; S_{serv_l} = \sum_{i=1}^{5} S_{serv_{il}}. \quad (10)$$

After that, the total levels of service importance and infrastructure levels are determined using the formulas:

$$S_{serv_i s} = \sum_{i=1}^{5} S_{serv_i}, \; S_{serv_l s} = \sum_{l=1}^{7} S_{serv_l}. \quad (11)$$

Below are the weighting factors for services (αS_{serv_i}) and infrastructure levels (αS_{serv_l}), which are determined by the formulas:

$$\alpha S_{serv_i} = \frac{S_{serv_i}}{S_{serv_i s}}, \quad (12)$$

where i=1,...,5;

$$\alpha S_{serv_l} = \frac{S_{serv_l}}{S_{serv_l s}}, \quad (13)$$

where l=1, ...,7.

Services and resources are then ranked by specific weights from highest to lowest to determine the most significant service/infrastructure levels 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 values of the integral indicator are determined:

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

$$IS_{serv\_rel} = \frac{IS_{serv\_abs} - S_{serv_{il}}\min}{S_{serv_{il}}\max - S_{serv_{il}}\min}, \quad (14)$$

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

The *overall integrated indicator of the current level of information security* in the analyzed security system is formed using the additive convolution of individual absolute integral indicators and the multiplicative convolution of individual relative integral indicators.

The additive integrated indicator of the current level of information security in the security system is calculated as:

$$IS_{add} = IS_{\inf\_abs} + IS_{ISO\_abs} + IS_{serv\_abs}. \quad (15)$$

The multiplicative integrated indicator of the current level of information protection in the security system is calculated as:

$$IS_{mult} = IS_{\inf\_rel} + IS_{ISO\_rel} + IS_{serv\_rel} \cdot (16)$$

Thus, the proposed general integrated assessment of system security shows that the closer the value of the relative indicator is to 1, the higher the influence of the relevant factors on information security in the security system.

In general, the presented mathematical apparatus allows to increase the level of objectivity of the assessment of "possible" targeted (mixed) attacks on the elements of the CIF infrastructure of both the first (physical systems) platform and the second (management systems) platform. In addition, a timely assessment of the current level of "capabilities" of the information protection system to resist (assessment of the availability of special mechanisms) targeted attacks on the elements of the CIF infrastructure is provide.

6. Assessment of the generalized effectiveness of security mechanisms based on the use of post-quantum algorithms

The constructed mathematical apparatus for forming integral indicators of the level of security and protection of critical infrastructure objects creates the basis for further development of methods for assessing the state of cyber defense. It is advisable to move from the analysis of generalized indicators of information security to assessing the effectiveness of protection mechanisms in the conditions of post-quantum threats. Further development of the obtained results consists in assessing the generalized effectiveness of security mechanisms taking into account the use of post-quantum algorithms that integrate means of noise-resistant coding into crypto-code structures. This approach ensures increased resistance of information and communication systems to quantum attacks, reduces the risk of data compromise and contributes to the formation of an adaptive and long-term protected cyberspace of critical infrastructure.

Table 2 presents the results of studies on the use of various noise-resistant codes in crypto-code constructions [13].

Table 2 – **The relationship between time and the level of information confidentiality**

Information security level	Information security time	Crypto-code constructions on corresponding codes
Critical	up to 1 year	MEC+Error-correcting codes
High	up to 1 month	MEC
Medium	up to 1 hour	EC
Low	up to 10 minutes	EC
Very low	up to 1 minute	LDPC

As can be seen from Table 2, which presents the relationship between the degree of information secrecy, the duration of its security preservation and the crypto-code constructions used, with the increase in the criticality of information, the requirements for its protection and the complexity of the mechanisms used increase. For critical data, it is advisable to use modified elliptic schemes (MEC) in combination with lossy codes that provide a long stability time, while for less important data, it is sufficient to use elliptical schemes (EC) or LDPC codes. This approach will allow to timely ensure the required level of security, taking into account the degree of information confidentiality and/or safe time, which is necessary for the provision of security services in multi-circuit information protection systems.

Table 3 shows the comparative characteristics of the use of cryptographic code structures in the post-quantum period, taking into account integration with various standards of wireless and mobile Internet technologies, as well as taking into account the criticality (degree of secrecy) of information. In other words, each technology listed in Table 3 is evaluated by how effectively it provides a certain “security service” – confidentiality, integrity, availability, authentication or affiliation.

Table 3 – **Comparison of wireless and mobile Internet technologies**

Technologies	Provision of security services					Information classification (βi)				
	A_i^C	A_i^I	A_i^A	A_i^{Au}	A_i^{Inv}	1,0	0,75	0,5	0,25	0,01
LTE (4G), LTE (5G)	–	–	+	–/+	–/+	–	–	–	–	–
IEEE 802.11 ac (WiFi 5)	–	–	+	–/+	–/+	–	–	–	–	–
IEEE 802.11ax, Wi-Fi 6+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE 802.16+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE802,16 м (WiMAX2)	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE 802.15.1Bluetooth 5+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE 802.15.4+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
Mobile technologies + CCC based on EC (MEC)	+	+	+	+	+	+	+	+	+	+

Technologies	Provision of security services					Information classification (βi)				
	A_i^C	A_i^I	A_i^A	A_i^{Au}	A_i^{Inv}	1,0	0,75	0,5	0,25	0,01
Mobile technologies + Hybrid Crypto-Code Constructions (HCCC) based on EC (MEC)	+	+	+	+	+	+	+	+	+	+
Mobile technologies + CCC based on LDPC codes	+	+	+	+	+	–	–	+	+	+

Table 3 shows a comparison of different wireless and mobile Internet technologies in terms of the level of security services and the ability to classify information by the security coefficient β_i.

From the analysis of Table 3, it is clear that traditional wireless standards (LTE, Wi-Fi 5, WiMAX, etc.) provide only a limited level of security, especially for data with a high or critical degree of secrecy. Their capabilities are mainly suitable for processing information of medium or low importance.

Instead, the combination of mobile technologies with crypto-code constructions, in particular, based on elliptic schemes (EC) or LDPC codes, provides a full range of security services for all categories of data, including critical ones. Hybrid crypto-code constructions (HCCC) based on EC demonstrate particularly high results, which guarantee the maximum level of cyber resilience.

Thus, the key direction for increasing the effectiveness of information protection in critical infrastructure networks is the integration of mobile technologies with post-quantum crypto-code methods.

To assess the comprehensive indicator of the effectiveness of security mechanisms based on post-quantum algorithms, reference tables were developed that allow you to identify the ranges of change of the necessary parameters and determine them in conditional scores. This method allows you to obtain quite adequate assessment results, and in addition, combine them with the results of accurate calculations for individual specific parameters.

Reference tables 4-12 show the parameters that are taken into account in the integrated indicator of functional efficiency of the intelligent multi-circuit system for protecting the elements of the CIF structure.

Table 4 – **Cost of implementing a targeted attack**

Scores	Parameter description
1	Very high cost
2	High cost
3	Medium cost
4	Low cost
5	Very low cost

Table 5 – **Рівень критичності атаки**

Scores	Parameter description
1	Critical
2	High
3	Medium
4	Low
5	Very low

Table 6 – **Level of computational complexity of the attack**

Scores	Parameter description
1	Very high
2	High
3	Medium
4	Low
5	Very low

Table 7 – **Attacker resource level**

Scores	Parameter description
1	Vandal resources
2	Resources of crime, competitors, hackers
3	Cybercriminal resources
4	State resources (special services)
5	Unlimited resources

Table 8 – **level of information confidentiality**

Scores	Parameter description
1	Very low
2	Low
3	Medium
4	High
5	Critical

Table 9 – **Час безпеки інформації**

Scores	Parameter description
1	Up to 1 minute
2	Up to 10 minutes
3	Up to 1 hour
4	Up to 1 month
5	Up to 1 year

Table 10 – **Security mechanisms/level of resilience**

Scores	Parameter description
1	symmetric (K=128 bits)/ 1 level
2	symmetric (K=256 bits)/level 2
3	symmetric (AES, K=128 bit)/ level 3
4	asymmetric, symmetric (AES, K=256 bit)/ level 4
5	post-quantum

Table 11 – **Data transmission technologies + cryptosystems**

Scores	Parameter description
1	IEEE 802.16+KNX (WSN)
2	IEEE802,16 м (WiMAX2)
3	IEEE 802.15.1Bluetooth 5+KNX (WSN)
4	IEEE 802.15.4+KNX (WSN)
5	Mobile technologies + CCC based on EC (MEC)
6	Mobile technologies + HCCC based on EC (MEC)
7	Mobile technologies + CCC based on LDPC codes
8	Gigabit Ethernet+(WSN)
9	10 Gb Ethernet+ (WSN)
10	40 Gb Ethernet+ (WSN)

Table 12 – **Послуги безпеки**

Scores	Parameter description
1	Possession
2	Possession, availability
3	Possession, availability, authenticity
4	Possession, availability, authenticity, integrity
5	Possession, availability, authenticity, integrity, confidentiality

Table 13 shows the generalized effectiveness of security mechanisms based on the integrated indicator of the assessment of the flow state of security of elements of critical infrastructure facilities.

Table 13 – **Generalized effectiveness of security mechanisms**

Technology	Conditional scores									
	group								Generalized efficiency index	Relative efficiency,%
	1	2	3	4	5	6	7	8		
IEEE 802.16+KNX (WSN)	2	4	3	2	3	3	3	4	5184	3,4
IEEE802,16м (WiMAX2)	1	5	1	1	2	2	1	2	40	0,26
IEEE 802.15.1Bluetooth 5+KNX (WSN)	2	4	3	2	3	3	3	3	3888	2,5
IEEE 802.15.4+KNX (WSN)	2	4	3	2	3	3	3	3	3888	2,5
Mobile technologies + CCC based on EC (MEC)	3	3	4	4	4	4	4	5	46080	32
Mobile technologies + HCCC based on EC (MEC)	5	1	5	5	5	5	5	5	78125	52,9
Mobile technologies + CCC based on LDPC codes	2	4	3	3	3	3	3	4	7776	5
Gigabit Ethernet+(WSN)	2	4	3	2	3	3	2	3	2592	1,7
10 Gb Ethernet+ (*WSN*)	2	4	3	2	3	3	2	3	2592	1,7
40 Gb Ethernet+ (*WSN*)	2	4	3	2	3	3	2	3	2592	1,7
Total:									152757	100

Note: Group: 1 – cost of implementing a targeted attack; 2 – attack criticality level; 3 – level of computational complexity of the attack; 4 – attacker's resource level; 5 – level of information confidentiality; 6 – information security time; 7 – security mechanisms /level of resilience; 8 – security services.

As can be seen from Table 13, the proposed approach allows obtaining a fairly adequate result. It is seen that today the most effective in terms of the totality of the above indicators is the use of post-quantum

algorithms - crypto-code structures based on elliptical codes (EC). The best indicator of the effectiveness of the intelligent multi-circuit security system CIF showed the use of hybrid crypto-code structures based on modified EC (MEC) with damage (damage codes). This approach provides countermeasures in the conditions of the emergence of a full-scale quantum computer and unlimited resources of terrorists and cybercriminals.

Discussion of results

The obtained research results demonstrate a systematic approach to assessing and improving the level of cyber security of critical infrastructure facilities in the context of post-quantum challenges. Based on a unified classifier of target threats, a formalization of potential attack scenarios was carried out, which allowed creating a consistent model of threat detection and analysis for various components of the CIF. The constructed model of the implementation of cyber threats and corresponding protection mechanisms made it possible to form a logical structure of interaction between security levels and information resources, taking into account the specifics of the multi-level architecture of modern cyber-physical systems.

The developed multi-circuit intelligent anti-terrorist protection system has demonstrated effectiveness in the context of adaptive response to complex combined attacks, which reflects the trend towards the integration of artificial intelligence into critical infrastructure security systems. The proposed methodology for assessing the state of the CIF security level provides the possibility of dynamic monitoring of the streaming state of cyber defense based on integrated indicators formed taking into account the interaction of technical, organizational and information factors.

The mathematical apparatus of forming integral indicators allowed to quantitatively assess the security status of the facility and provide a comparative analysis of different security systems. Particular attention was paid to the construction of a generalized integrated indicator of the level of information security, which serves as the basis for further optimization of protection mechanisms.

The assessment of the effectiveness of security mechanisms taking into account the use of post-quantum algorithms showed that the implementation of crypto-code structures based on noise-resistant codes, in particular LDPC and ECC, provides a significant increase in resistance to quantum attacks. Therefore, the results confirm the feasibility of a comprehensive approach to cyber security that combines classical and post-quantum cryptography tools, intelligent threat analysis modules, and adaptive security management circuits.

Thus, the proposed model of integrated assessment of the level of cybersecurity is an effective tool for supporting decision-making on the modernization of critical infrastructure protection systems in the face of growing post-quantum risks.

Conclusions

As a result of the research, a methodology for assessing the level of security of critical infrastructure facilities (CIF) was developed, which is based on a combination of mathematical, expert and intellectual methods of risk analysis. The proposed approach is based on a synergistic threat model that takes into account the categories of attackers, their goals, resources and capabilities, as well as the nature of the impact on information assets. This approach allows for a comprehensive coverage of the entire spectrum of potential cyber threats and ensures an adaptive response of the security system to changes in the operating environment.

The CIF security level assessment obtained as a result of the audit made it possible not only to determine the most valuable information assets, but also to identify the effectiveness of existing protection measures, identify vulnerabilities and risk areas that require priority modernization. Based on the analysis, recommendations were developed to increase the level of cyber security, aimed at optimizing security policies, increasing resistance to targeted attacks and reducing the consequences of possible incidents.

The key result of the research is confirmation of the need to implement intelligent multi-circuit information protection systems that are capable of real-time monitoring of the security flow state, conducting correlation analysis of events, and dynamically responding to anomalies. Such systems, built on the basis of post-quantum cryptographic algorithms and crypto-code structures using noise-resistant codes (LDPC, ECC, etc.), provide the necessary level of long-term information security even in conditions of quantum threats.

The results obtained confirm the feasibility of moving to an integrated approach to cybersecurity assessment, which combines technical, organizational and analytical mechanisms, forming a holistic risk management model for critical infrastructure.

Prospects for further research lie in the development of adaptive cyber threat prediction systems using machine learning and analysis of behavioral attack patterns, improving streaming security assessment models through integration with IoT and artificial intelligence, as well as expanding post-quantum cryptographic protection methods using new jamming-resistant codes. The results obtained form the basis for the development of reliable and quantum-resistant security systems of the future.

REFERENCES

1. Makrakis, G. M., Kolias, C., Kambourakis, G., Rieger, C. and Benjamin, J. (2021), "Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents", *IEEE Access,* Vol. 9, doi: 10.1109/ACCESS.2021.3133348
2. Bajwa, A., Tonoy, A. Al R., Rana, S., and Ahmed, I. (2025), "Cybersecurity in industrial control systems: a systematic literature review on AI-based threat detection for Scada and IoT networks", *ASRC Procedia: Global Perspectives in Science and Scholarship*, Vol. 1(01), pp. 01-15, https://doi.org/10.63125/1cr1kj17
3. Wolfmayr, M. and Viljakainen, T. (2025), "A review on post-quantum cryptography and related cyber threats for critical infrastructures", *Jamk Arena Pro,* URL: https://urn.fi/urn:nbn:fi:jamk-issn-2984-0783-225
4. Brancati, F., Mongelli, D., Mariotti, F. and Lollini, P. (2025), "A cybersecurity risk assessment methodology for industrial automation control systems", *International Journal of Information Security,* 24:76, https://doi.org/10.1007/s10207-025-00990-9
5. Prokopovych-Tkachenko, D. I., Khrushkov, B. S. and Derkach, Y. O. (2025), "Post-quantum threats to information security: challenges at the global and national levels", *Systems and Technologies*, Vol. 69(1), pp.118-123, https://doi.org/10.32782/2521-6643-2025-1-69.14
6. "Models of socio-cyber-physical systems security": monograph (2023) / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others, *Kharkiv: PC TECHNOLOGY CENTER*, 168 p., DOI: https://doi.org/10.15587/978-617-7319-72-5
7. Framework for assessing the current state of protection, URL: https://skl.sspu.sumy.ua/
8. Yevseiev, S., Korolyov, R., Tkachov, A., Laptiev, O., Opirskyy, I. and Soloviova, O. (2020), "Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period", *International Journal of Advanced Trends in Computer Science and Engineering,* Vol. 9, No 5, pp. 8725-8729, https://doi.org/10.30534/ijatcse/2020/261952020
9. Aragon, N., Barreto, P. S. L. M., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.-C., Gaborit, P., Gueron, S., Güneysu, T., Melchor, C. A., Misoczki, R., Persichetti, E., Sendrier, N., Tillich, J.-P. and Zémor, G. (2018), "BIKE: Bit Flipping Key Encapsulation", *Submitters, Amazon Web Services, Intel Corporation*, *Worldline,* 54 p. URL: http://bikesuite.org/files/BIKE.pdf
10. Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G. and Stehlé, D. (2018), "CRYSTALS – Kyber: a CCA-secure module-lattice-based KEM", *IEEE European Symposium on Security and Privacy*, DOI: 10.1109/EuroSP.2018.00032
11. Smith, B. (2018), "Pre- and post-quantum Diffie–Hellman from groups, actions, and isogenies" / Book Chapter, *International Workshop on the Arithmetic of Finite Fields,* pp. 3-40, URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://inria.hal.science/hal-01872825/document
12. Hamming Quasi-Cyclic (HQC) An IND-CCA2 Code-based Public Key Encryption Scheme (2022), *NIST 4 th PQC Standardization Conference*, URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/ https://csrc.nist.gov/csrc/media/Presentations/2022/hqc-update/images-media/session-4-gaborit-hqc-pqc2022.pdf
13. Yevseiev, S., Havrylova, A., Korol, O., Dmitriiev, O., Nesmiian, O. and Yufa, Y. (2022), "Research of collision properties of the modified UMAC algorithm on crypto-code constructions", *EUREKA: Physical Sciences and Engineering*, No 1, pp. 34–44, DOI:10.21303/2461-4262.2022.002213

Received (Надійшла) 31.10.2025
Accepted for publication (Прийнята до друку) 14.11.2025

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

Меленті Євген Олександрович – кандидат технічних наук, доцент, перший проректор, Національна академія Служби безпеки України, Київ, Україна;
Yevhen Melenti – PhD, associate professor, First vice-rector, National Academy of Security Service of Ukraine, Kyiv, Ukraine;
e-mail: melenty@ukr.net; ORCID Author ID: https://orcid.org/0000-0003-2955-2469;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57217492946.

Мурр П'єр – доцент кафедри комп'ютерної інженерії, Міжнародний університет науки і технологій у Кувейті, Ардія, Кувейт;
Pierre Murr – PhD, Assistant professor, Computer Engineering Department, International University of Science and Technology in Kuwait, Ardiya, Kuwait;
e- mail: murrpierre@gmail.com; ORCID Author ID: https://orcid.org/0009-0007-4094-0223.

Аксьонова Ірина Вікторівна – кандидат економічних наук, доцент, старший дослідник, доцент кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Iryna Aksonova – Candidate of Economic Science, Associate Professor, Senior researcher, Associate Professor of Cyber Security Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: ivaksyonova@gmail.com; ORCID Author ID: https://orcid.org/0000-0003-2605-0455;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57206727489.

Букатич Ілля Вадимович – аспірант кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Illia Bukatych – PhD student of Cyber Security Department, National Technical University "Kharkiv polytechnic institute", Kharkiv, Ukraine;
e-mail: illia.bukatych@gmail.com; ORCID Author ID: https://orcid.org/0009-0007-4695-073X;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=59490108100.

Сітченко Олександр Анатолійович – аспірант кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;

Oleksandr Sitchenko – PhD student of Cyber Security Department, National Technical University “Kharkiv polytechnic institute”, Kharkiv, Ukraine;
e-mail: oleksandr.sitchenko@cs.khpi.edu.ua; ORCID Author ID: https://orcid.org/0009-0007-8756-398X.

ІНТЕГРОВАНА ОЦІНКА РІВНЯ КІБЕРЗАХИЩЕНОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В ПОСТКВАНТОВОМУ СЕРЕДОВИЩІ

Є.О. Меленті, П. Мурр, І.В. Аксьонова, І.В. Букатич, О. А. Сітченко

Анотація. Актуальність дослідження зумовлена зростанням складності кіберзагроз у постквантовому середовищі, розвитком квантових обчислювальних технологій та інтелектуалізацією процесів управління й оброблення даних. В умовах поширення гібридних і синергетичних атак, що поєднуються з методами соціальної інженерії, традиційні підходи до оцінювання безпеки об’єктів критичної інфраструктури (ОКІ) стають малоефективними. Це потребує впровадження інтегрованої методики оцінки рівня кіберзахищеності, здатної адаптивно відображати реальний стан безпеки та враховувати вплив постквантових загроз. **Предметом дослідження** є процес інтегрованої оцінки рівня кіберзахищеності ОКІ в постквантовому середовищі з використанням математичних та аналітичних методів. **Метою статті** є розроблення методики інтегрованої оцінки рівня захищеності ОКІ в постквантовому середовищі з урахуванням сучасних гібридних та синергетичних кіберзагроз. **Отримані результати**. Запропоновано методику оцінювання рівня захищеності на основі синергетичної моделі загроз, що враховує категорії зловмисників, їх цілі, ресурси та можливості. Розроблено математичну формалізацію уніфікованого класифікатора кіберзагроз, який формує кортежі з урахуванням ознак гібридності, синергізму та соціоінженерних факторів. Сформовано математичний апарат для моделювання реалізації кіберзагроз і визначення рівня стійкості кіберсистем ОКІ в постквантовому середовищі. **Висновки**. Оцінка захищеності ОКІ дає змогу визначити критично важливі інформаційні активи, оцінити ефективність засобів захисту та виявити вразливі елементи. Результати дослідження підтверджують доцільність упровадження інтелектуальних багатоконтурних систем захисту на основі постквантових алгоритмів для забезпечення належного рівня кіберстійкості в постквантовому середовищі.

Ключові слова: постквантові загрози, синергетична модель кіберзагроз, інтегрований показник безпеки, об’єкт критичної інфраструктури, інтелектуальна багатоконтурна система захисту.