

Critical Infrastructure Resilience and Cybersecurity of Information Management Systems

Oleksandr Dodonov¹, Olena Gorbachyk¹, Maryna Kuznietsova¹

¹Institute for Information Recording of the National Academy of Sciences of Ukraine, Kyiv, 03113, Ukraine

Abstract

This article defines the concepts of resilience and security in critical infrastructures, highlighting their dependence on the cybersecurity of information systems. The organizational measures to improve the security of critical infrastructures in the world and in Ukraine are considered: ensuring the resilience of critical infrastructures, existing international approaches and standards, technologies and means of ensuring cybersecurity. The methodological foundations for analyzing, assessing and managing security risks, including cybersecurity risks in automation complexes, automated process control systems of industrial enterprises, and information management systems of critical infrastructures in various industries, are investigated. The tasks of risk assessment and security of critical infrastructures are formulated. Theoretical and multiple models are proposed, the application of which allows analyzing the existing interactions of systems and subsystems of critical infrastructure under conditions of uncertainty, the emergence of a security deficit due to the negative impact of factors of different nature and the interaction of critical infrastructure components.

Keywords

critical infrastructure resilience, information management system, functional resilience, survivability, cybersecurity, risks


1. Introduction


Critical infrastructures are vital systems whose accidents and malfunctions cause damage to the economy, the environment, and human health and life. These systems include energy networks, transportation systems, telecommunication networks, banking systems, water supply and sewage, heating systems, etc. In the current hybrid war, the full functioning of critical infrastructures is under threat. In 2022, Ukraine faced approximately 7,000 cyberattacks on its information infrastructure. From February 24 to the end of 2022, the Ukrainian government's computer emergency response team CERT-UA handled 2194 cyber incidents, of which 120 concerned the financial sector, 156 commercial organizations, and 92 telecommunications and software development sectors [1]. Cyberattacks on critical infrastructure are becoming more sophisticated and complex. At the end of 2022, Mandiant [2] analyzed a cyber-physical attack by the Sandworm group of Russian hackers on a Ukrainian critical infrastructure facility. The attack used a new technique (a variant of the CADDYWIPER malware in the victim's IT environment) that affected industrial control systems and operational technologies, leading to an unplanned power outage during missile strikes on Ukraine.


The evolution of cyberattacks and the growing trend of attacks on control information systems threaten the full functioning of critical infrastructures in a hybrid war. Protecting critical infrastructure from cyberattacks is a strategically important task that requires the implementation of comprehensive cybersecurity solutions. The risk of harm to people, society, and the environment must be reduced to an acceptable level.


In the context of military operations, Ukraine pays serious attention to the protection and security of critical infrastructures. The country has enacted a series of legislative and regulatory measures that define the roles and responsibilities of government agencies in this area and related fields. These measures also outline the specifics of ensuring the protection and safe operation of

ITS-2023: Information Technologies and Security, November 30, 2023, Kyiv, Ukraine

 dodonovua@gmail.com (O. Dodonov); bges@ukr.net (O. Gorbachyk); marglekuz@gmail.com (M. Kuznietsova)

 0000-0001-7569-9360 (O. Dodonov); 0000-0001-8492-4478 (O. Gorbachyk); 0000-0001-6054-418X (M. Kuznietsova)

 © 2023 Copyright for this paper by its authors.

 Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

critical infrastructure facilities and systems. However, it is still premature to speak of a comprehensive, national-level approach to managing the protection and security of the entire network of critical systems, facilities, and resources, considering their interconnectedness and mutual dependencies. There is no mechanism for preventing possible crises related to the functioning of information and control systems of critical infrastructures. There is no clear interaction and coordination of actions of the responsible state authorities to avoid emergencies in critical infrastructures, to involve existing (already applied) practices of business entities to improve the security and stability of critical infrastructures.

2. Basic concepts and definitions

The resilience of critical infrastructure is a property that characterizes its ability to adapt to aggressive operating conditions, recover from disruptions while minimizing negative impacts on vital social functions, economic activity, public health and safety, or the environment. *Critical infrastructure security* means independence from unacceptable risk, infrastructure protection, guaranteeing its functionality, continuity of operation, integrity and resilience, i.e. ensuring a state of infrastructure where the risk of harm to a person, society, or country is reduced to an acceptable level.

In our opinion, the emergence of the term "resilience" is related to the growing security risks of critical infrastructures, the permanent change in the threat landscape, the emergence of a cross-border and interdependent network of vital services using key critical infrastructure facilities in different countries [3], and the understanding of the catastrophic consequences of cascading accidents that can lead to far-reaching and long-term negative impacts on the lives of people, societies, and countries.

Information and control systems (ICS) are part of any critical infrastructure and are the main information asset of critical infrastructure. These systems collect, process, store and transmit information to ensure the management functions, sustainable operation and development of critical infrastructure. ICS are characterized by the criticality of the tasks to be solved, distributed nature, complexity of hardware and architectural implementation, strict requirements for the management time cycle, etc. The characteristics of critical infrastructure and ICS, recorded at certain points in time by monitoring tools, describe the system states. Formally, the changes in system states can be represented as a tuple:

$$\begin{aligned} < \bar{\theta}^{(1)} = \left(\theta_1^{(1)}(t_1), \theta_2^{(1)}(t_1), \dots, \theta_k^{(1)}(t_1) \right), \\ \bar{\theta}^{(2)} = \left(\theta_1^{(2)}(t_2), \theta_2^{(2)}(t_2), \dots, \theta_k^{(2)}(t_2) \right), \dots, \\ \bar{\theta}^{(n)} = \left(\theta_1^{(n)}(t_n), \theta_2^{(n)}(t_n), \dots, \theta_k^{(n)}(t_n) \right) >, \end{aligned}$$

where $\theta_i^{(n)}(t_n)$ is the i -th characteristic's value at the n -th time point t .

System evolution can be interpreted as transitions in a k -dimensional phase space. Evolution can lead to improvement or deterioration of the system's functioning and the emergence of new security risks, so it is necessary to have not only the means to detect incidents in critical infrastructures and report them, but also to reduce risks, so we need the means to manage the evolution of technical and sociotechnical systems.

One of the factors that negatively affect the functioning of critical infrastructure is *cyberattacks*, which are targeted or unintentional impacts on the computerized or automated components of the infrastructure through software or hardware. Depending on the peculiarities of the functioning of information systems, their information resources and data, cyberattacks can cause a breach of *confidentiality, integrity, availability* (or some combination thereof) of data, that may in some cases lead to a cascading effect in critical infrastructure. Therefore, the sustainable operation of critical infrastructure requires protection of its information infrastructure from cyberattacks.

The expansion of ICS functionality has contributed to the development of means of influencing these systems and to the growth of cyberattacks, the volume and sophistication of which have been

rapidly increasing lately. Cyberattacks are aimed primarily at destabilizing computer systems, destroying IT resources, disrupting access to services of government agencies, financial and business centers, and causing disruption to critical infrastructures, organizations and entire countries that rely on the Internet for their daily lives.

Today, there is no single standard and definition of cybersecurity. According to the International Standard ISO/IEC 27032, cybersecurity includes: network protection; endpoint protection; protection against social engineering methods; and relationship security, i.e. cybersecurity is aimed at protecting IT resources of critical infrastructure.

Analysis and assessment of critical infrastructure security and resilience should be multifactorial, as it is impossible to obtain a reliable security assessment without taking into account the mutual influence of infrastructure components, interpenetration of different infrastructures, human factor, reliability of ICS software and hardware, etc.

Cybersecurity, both as an academic field and as a practical discipline aimed at countering cyberattacks, encompasses a wide range of activities. These include securing operating systems and databases, developing and implementing technical information protection systems, providing antivirus protection, safeguarding web services and cloud systems, securing network communications, and creating methods to counteract malware. Additionally, it involves addressing the human factor, which remains one of the most common causes of information leakage, modification, or destruction. Cybersecurity is an integral part of the process of ensuring the information security of critical infrastructures. Decisions on the protection of information infrastructure interconnected with a particular critical infrastructure should be based on the analysis and assessment of risks and possible losses from the implementation of cyber threats.

Understanding the scale of possible damage to critical infrastructure in the event of a threat is based on an a priori assessment of the threat's potential. The risk to critical infrastructure is higher the greater the potential of the threat.

Usually, the threat potential is quantified a priori using expert assessment methods. If the threat δ^i is characterized by parameters $\{\delta_j^i\}$, $j = \overline{1, n}$, and each of them is evaluated by experts on a certain point scale, then the threat potential assessment can be a certain function $f = f(\delta_1^i, \delta_2^i, \dots, \delta_n^i)$, in particular, it can be the sum of the point estimates of the parameters, the weighted sum of the parameter estimates. When determining the threat potential, it is appropriate to take into account the fact that it may change over time, i.e. $f = f(\delta_1^i, \delta_2^i, \dots, \delta_n^i; t)$. Assessment of the threat potential over time is an important characteristic, as it allows for more effective planning of critical infrastructure protection means and forces.

Quantitative and descriptive risk assessment allows for a quantitative assessment of the security level of information systems vulnerable to these risks within critical infrastructures and a quantitative assessment of the security level and a descriptive characterization of the effectiveness of existing methods of countering threats. In the future, it is possible to plan the necessary improvements to protection and cybersecurity systems through the introduction of new technologies or improving the efficiency of existing ones to achieve the required generally accepted level of security for a particular critical infrastructure.

Data analysis systems for monitoring the state of critical infrastructure facilities and systems as part of the ICS should be configured to detect unexpected behavior of vulnerable systems identified for monitoring, ensuring the prevention of threats or activation of technologies, processes, and control influences to avoid critical infrastructure accidents. Each incident that occurs in critical infrastructure should be recorded and analyzed to understand what threats have occurred and how well cybersecurity measures have countered them.

It is clear that critical infrastructures require an integrated approach to ensuring their security, which involves the mutually coordinated adoption and implementation of management and technological decisions on all aspects of security.

3. Problematic situation

Today, the biggest corporate risks in the United States, Australia, India, Japan, Germany, and the United Kingdom, according to the Allianz Risk Barometer [4], are cyber incidents, data leaks (59%),

attacks on critical infrastructure or physical assets (53%), and increased ransomware attacks (53%). Automated control systems of critical infrastructure entities that use IoT applications pose a serious threat to the cybersecurity of important critical infrastructure facilities. The result of a cyberattack on critical information infrastructure can be catastrophic, leading to the destruction or loss of control over other critical infrastructures, transfer of control to a third party, rendering critical infrastructures inoperable, and jeopardizing the confidentiality of people's personal data.

In the EU, the main body responsible for achieving a high common level of cybersecurity is the European Union Agency for Cybersecurity ENISA. ENISA has developed a single pan-European concept of protection, Cyber Europe, which was adopted in 2009 and is updated every two years. Requirements for the protection of critical infrastructures are determined by the national legislation of individual EU member states, and critical infrastructure risk management in most European countries is also based on national programs.

The United Kingdom, for example, has a Risk Management Framework (RMF) based on the National Infrastructure Protection Plan (NIPP), which provides general guidance on security objectives, strategies, and sectors of coverage. Elements of critical infrastructure are physical, cyber and human resources. From the initial stage of establishing security objectives and facilities, the main stages used as evaluation criteria are the identification of infrastructure assets, risk assessment and analysis, implementation of risk management (including risk prioritization and risk control), and performance measurement. A process of periodic information exchange is carried out and feedback is provided between the stages of risk management. Tools, risk management methods, and protection methodologies are defined in accordance with the purpose they fulfill at each stage of the overall risk management.

In the United States, as part of the National Cyber Security Division (NCSA), there is a program to protect control systems and a special team to respond to cyber threats in industrial systems (ICS-CERT - Industrial Control Systems Cyber Emergency Response Team).

The European Commission has developed a global strategy for the protection of critical infrastructure (The European Program for Critical Infrastructure Protection) and proposed now the creation of a single structured incident response platform (Cybersecurity Crisis Response Framework). The platform will include national and cross-border operations centers that will detect and respond to cyber threats using modern technologies, including artificial intelligence (AI) and advanced data analysis, to identify and share timely warnings of cyber threats and cross-border incidents. The so-called European Cyber Shield will be created to effectively detect cyber threats - a pan-European infrastructure consisting of national and cross-border security operations centers (SOCs) for all EU countries.

Thus, an effective cybersecurity program should include people, processes, and technological solutions that together reduce the risk of disruption of critical infrastructure. Functional resilience and survivability of critical infrastructure and ICS, which are capable of providing timely response to threats, reporting incidents, and generating appropriate control actions, are essential conditions and factors for critical infrastructure security.

Today, certain methodological approaches to analyzing cybersecurity risks for technological processes and industrial enterprises in various industries have already been developed and implemented [5]. The gas and oil refining industries use the Cyber Process Hazard Analysis (Cyber PHA) approach, which is based on the classical approach to identifying, assessing and managing process risks and includes aspects related to cybersecurity risks [5]. For example, Shell has jointly used HSSE (Health, Safety, Security and Environment) risk assessment methods, traditional PHA assessment methods, and cybersecurity risk assessment methods to assess the factors that lead to a violation of the integrity of security functions due to cybersecurity threats (which are or may be present in software and hardware automation systems) [5].

International standards for cybersecurity risk analysis have been developed: ISO/IEC 27001 [6] - threat analysis; ISA TR84.00.09 [7] - threat analysis and cybersecurity risk assessment, description of cybersecurity requirements at all stages of the system life cycle; ISA/IEC 62443 [8] - building a secure process control system architecture at the automation and process control level. ISA/IEC 62443 proposes an integrated approach that involves the creation of a cybersecurity management system (CSMS) for an industrial facility, and the main components are risk analysis, risk elimination through CSM, control and improvement of the CSMS.

Ukraine's critical infrastructures have a rather complex structure of interconnections and mutual influences. The international standard for information security management ISO/IEC 27001 is mainly applied to critical infrastructures in Ukraine, and national recommendations are only being developed. The Government of Ukraine has approved the National Plan for the Protection and Ensuring the Security and Resilience of Critical Infrastructure, which provides, inter alia, monitoring critical infrastructure; assessing risks and threats; determining the procedure for interaction between critical infrastructure protection entities in crisis situations; ensuring the functioning of the information exchange system; and strengthening the resilience of critical infrastructure. Functionally stable management information systems with effective mechanisms for dynamic reconfiguration, reorganization, adaptation and recovery should play a significant role in maintaining the security of critical infrastructure. Recognized cybersecurity practices are already being used to minimize the risks and negative consequences of cyberattacks: network security, cloud security, application security, operational security, business continuity, threat awareness programs, etc.

4. The task of assessing the security and risks of critical infrastructures

Critical infrastructure can be viewed as a set of objects/systems $\{S_i\}_1$, their ICS and information subsystems for various purposes $\{I\&C_q^i\}_Q$ and r connections (interactions) $I(t)_r^{CI}(S_i \rightarrow S_j)$ between systems [9].

Interactions of this type exist at all levels of critical infrastructure, at the subsystem level, and \bar{S} at the system-subsystem level:

$$I(t)_r^{S_{ij}}(\bar{S}_{ik} \rightarrow \bar{S}_{lm}), \quad I(t)_r^{S_i}(S_i \rightarrow \bar{S}_{ik})$$

The main means of controlling the security of systems is ICS $\{I\&C_q^i\}_Q$, between the subsystems of which there is also an interconnection $I(t)_r^{I\&C_q}(\bar{S}_{ik} \rightarrow \bar{S}_{jl})$ [10].

For each critical infrastructure, the safety index $SI_{CI}(t)$ and reliability indicators $RI_{S_i}(t)$ are determined, and the cost of resources to improve the safety index and reduce risks is determined [9].

The ICS of critical infrastructure is usually characterized by survivability, functional safety $\{FSI_{I\&C}(t)\}$ and functional resilience. There is a relationship between the safety indicators $SI_{CI}(t)$ and $\{FSI_{I\&C}(t)\}$. The safety states $\{St_l^{S_i}(t)\}_L$ and $\{St_g^{S_{ij}}(t)\}_G$ characterize the system S_i and subsystem \bar{S}_{ij} .

The critical infrastructure security index $SI_{CI}(t)$ is consistent with the defined value if and only if the current risks $R_{CI}(t)$ are acceptable:

$$SI_{CI}(t) = SI_{CI}^{accept}(t) \Leftrightarrow R_{CI}(t) = R_{CI}^{accept}(t).$$

When current risks increase and do not meet the acceptable values, i.e. $R_{CI}(t) \notin \Upsilon_{R_{CI}^{accept}}$, where Υ is the set of acceptable risks, then the current critical infrastructure security indicator is not consistent with the corresponding value $SI_{CI}^{reg}(t)$, i.e. $SI_{CI}(t) \notin \Omega_{SI_{CI}^{accept}}(t)$.

The risks of critical infrastructure depend on local risks $R_{S_i}^{local}(t)$, which are identified at the stage of critical infrastructure development, and emergent risks $R_{CI}^{emerg}(t)$, which are caused by negative external influences between subsystems that make up the critical infrastructure. It is difficult to determine the probability and severity of emergent risks due to the insufficiency and inaccuracy of data for such analysis.

The security dependencies between critical infrastructure systems can be summarized as follows:

$$\{St_g^{S_i}(t), St_k^{S_j}(t), \mu(St_g^{S_i}(t), St_k^{S_j}(t)) \neq 0\},$$

where μ - a membership function that indicates the degree (level) of membership of an element in a set.

ICS are also characterized by risks that may be greater (less) than the acceptable risks of the ICS, i.e. $R_{I\&C_q^i}(t) <> R_{I\&C_q^i}^{accept}(t)$.

The security dependency between critical infrastructure and ICS can be summarized as follows:

$$\{St_g^{S_i}(t), St_k^{I\&C_q^i}(t), \mu(St_g^{S_i}(t), St_k^{I\&C_q^i}(t)) \neq 0\}.$$

There is a relationship between the risks $R_{I\&C_q^i}(t)$ and $R_{CI}(t)$, namely:

$$R_{I\&C_q^i}(t) \subseteq R_{CI}(t) \text{ and } R_{CI}(t) \subseteq R_{I\&C_q^i}(t).$$

Uncertainty in security and risk assessment is caused by the blurred boundaries of the critical infrastructure security problem, the complexity of the behavior of critical infrastructure components and the infrastructure itself, the uncertainty of the response of systems and subsystems to external influences, the emergence of critical infrastructure properties, and the low accuracy of security assessment models. This is compounded by the complex and dynamic nature of risks, the impossibility of exhaustive risk identification and classification, and the complexity of the nature of interactions between critical infrastructure components.

The Safety Model of critical infrastructure can be formally represented in a set-theoretic form:

$$SM = \{\{S_{ij}\}_{IJ}, \{I(t)_h^{CI}(S_i \rightarrow S_j)\}_H, \{St_g^{S_{ij}}\}_G, \{SF_d\}_D, \{P_h^{parametr}(S_i)\}_H, \{R_j\}_J\}$$

$$SI_{S_i}(t) = R_j(SM),$$

where $\{S_{ij}\}_{IJ}$ - set of critical infrastructure systems (subsystems);

$\{I(t)_h^{CI}(S_i \rightarrow S_j)\}_H$ - set of connections between critical infrastructure systems (subsystems);

$\{St_g^{S_{ij}}\}_G$ - set of security states of critical infrastructure systems;

$\{SF_d\}_D$ - set of security factors;

$SI_{S_i}(t)$ - set of security indicators for critical infrastructure systems;

$\{P_h^{parametr}(S_i)\}_H$ - set of security state parameters that describe the critical infrastructure system (e.g., limit state parameters);

$\{R_j\}_J$ - set of relations between the above sets;

H - set of hazards for critical infrastructures.

The set $H_{I\&C}$ of typical hazards for ICS includes the following elements:

$$H_{I\&C} = \{h_{I\&C}^1, h_{I\&C}^2, h_{I\&C}^3, h_{I\&C}^4\},$$

where $h_{I\&C}^1$ - physical failures of ICS hardware;

$h_{I\&C}^2$ – decrease in the quality of ICS functioning (service failures);

$h_{I\&C}^3$ – external influences on ICS;

$h_{I\&C}^4$ – design errors.

The critical infrastructure security model is a formalized link between the parameters of the model itself and the critical infrastructure security indicator.

The critical infrastructure security model should integrate all the input data available for research, should take into account the dynamic nature of risks, changes that occur in the process of evolution of critical infrastructure and the life cycle of information systems, should also take into account the interactions of systems/subsystems in critical infrastructure, security factors and allow determining the security indicator of systems in critical infrastructure and critical infrastructure as a whole. When studying the security of critical infrastructure, we understand the interactions between systems as the ability of the system S_i (the object of influence) to change the security state of the system S_j (the subject of influence). The impact (physical, informational, organizational, etc.) can be represented as $\{I(t)_h^{CI}(S_i \rightarrow S_j)\}_H$.

Interactions at different levels of critical infrastructure between its components (systems/subsystems) are an inherent characteristic of any critical infrastructure. If the degree of its overall impact on other critical infrastructure components is determined for each system/subsystem, then by ranking the values of the overall impact by magnitude, it is possible to identify the system whose security state is crucial for the state of other systems.

It should be noted that interactions, on the one hand, increase the infrastructure's resilience to security factors, and on the other hand, complicate the forecasting of states and lead to the emergence of new risks in critical infrastructures. Changes in the magnitude and direction of the impact between systems can lead to accidents and disruptions in the operation of critical infrastructure. Statistics on disruptions and accidents in critical infrastructures show that physical and information impacts are the most significant in terms of security. Thus, in 2023, the System for Detecting Vulnerabilities and Responding to Cyber Incidents and Cyber Attacks (CBB - a set of software and hardware tools that provide round-the-clock monitoring, analysis and transmission of telemetry information about cyber incidents and cyber attacks that have occurred or are occurring at cyber security facilities and may have a negative impact on their sustainable functioning) processed about 18 billion events, including 133 million suspicious and 148 million critical information security events [11]. The number of devices connected to global networks, edge processing and analytics, distributed cloud computing, and the Everything-as-a-Service (EaaS) approach are becoming commonplace in critical infrastructures, and this significantly reduces the effectiveness of security measures such as physical network security models and perimeter organization.

The formalized statement of the task of ensuring the security of critical infrastructure (the security indicator is consistent with the defined one) will be as follows:

$$\left(\frac{\text{critical}}{\text{infrastructure}}\right) = \left\{ \{S_i\}_I, \{I\&C_q\}_Q, \{\bar{S}_{ij}\}_{IJ}, I(t)_h^{CI}(S_i \rightarrow S_j), I(t)_h^{S_{ij}}(\bar{S}_{ik} \rightarrow \bar{S}_{lm}), I(t)_h^{S_i}(S_i \rightarrow \bar{S}_{ik}) \right\}$$

$$\exists SI_{CI}(t) \notin \Omega_{SI_{CI}^{accept}(t)}, \exists R_{CI}(t) \notin \Upsilon_{R_{CI}^{accept}}, \exists C_{CI}(M_{CI}) \in \Omega_{accept} ;$$

$$I\&C_q = \left\{ \{\bar{S}_{ij}\}, I(t)_h^{I\&C_q}(\bar{S}_{ik} \rightarrow \bar{S}_{jl}) \right\}, \exists SI_{I\&C_q}(t) \notin \Omega_{SI_{I\&C_q}^{accept}(t)}, \exists R_{I\&C_q}(T) \notin \Upsilon_{R_{I\&C_q}^{accept}(t)}$$

it is necessary to ensure an acceptable level of critical infrastructure security indicator by identifying, assessing and reducing emergent risks through diversification of systems (subsystems) in critical infrastructure and redistribution of resources, ensuring that emergent risks are reduced to an acceptable level:

$$CI^* = \left\{ \{S_i^*\}_I, \{\bar{S}_{ij}^*\}_{IJ}, I^*(t)_h^{CI} (S_i^* \rightarrow S_j^*), I^*(t)_h^{S_{ij}^*} (\bar{S}_{ik}^* \rightarrow \bar{S}_{lm}^*), I^*(t)_h^{S_i^*} (S_i^* \rightarrow \bar{S}_{ik}^*) \right\},$$

$$\exists SI_{CI^*}(t) \in \Omega_{SI_{CI^*}^{accept}(t)}, \exists R_{CI}(t) \in \Upsilon_{R_{CI}^{accept}}, \exists C_{CI^*}(M_{CI^*}) \in \Omega_{accept} ;$$

$$I\&C_q^* = \left\{ \{\bar{S}_{ij}^*\}, I^*(t)_h^{I\&C_q} (\bar{S}_{ik}^* \rightarrow \bar{S}_{il}^*) \right\}, \exists SI_{I\&C_q^*}(t) \in \Omega_{SI_{I\&C_q^*}^{accept}(t)}, \exists R_{I\&C_q^*}(T) \in \Upsilon_{R_{I\&C_q^*}^{accept}(t)}.$$

Reducing infrastructure risks should not lead to increased risks for the ICS and, accordingly, a decrease in its functional security. It should be noted that a set of risk reduction measures (diversification and redistribution) in critical infrastructures is limited by resources $C_{CI}(M_{CI}) \in \Omega_{accept}$.

6. Critical infrastructure security risk management

It is clear that it is desirable for critical infrastructures to prevent risks by implementing certain preventive measures and having worked out scenarios of actions in the event of a risk situation, i.e. to be what is called "proactive".

The process of making and implementing management decisions aimed at reducing the likelihood of hazardous events and minimizing possible losses associated with them is called risk management. The main features of risk management in critical infrastructures include: a significant number of stakeholders, a variety of approaches to risk management, uncertainty of ergonomic risks, and interconnectedness of the security states of critical infrastructure components.

The direction and priorities for steady progress in the dynamics while improving the security of critical infrastructures are determined by long-term solutions. For example, the introduction of the Zero Trust principle, which offers real-time detection of abnormal behavior regardless of the location of the threat, will allow you to develop a strategy, plan and architecture to reduce risks. Short-term solutions for protection and countermeasures turn long-term solutions into concrete ongoing actions.

The following stages of risk management can be distinguished for critical infrastructures:

- a priori hazard analysis to identify critical infrastructure assets that are most important for infrastructure security;
- identification of the types of impacts between systems that make up the critical infrastructure;
- identification of emergent risks associated with negative interactions between critical infrastructure systems;
- risk analysis;
- assessment of the emergent risk associated with the types of impacts, in particular, assessment of the occurrence of a hazardous event (accident, failure) related to the interaction of critical infrastructure systems, assessment of the severity of the consequences of risk events for infrastructure security;
- selection of a risk management strategy;
- implementation of a security scenario taking into account the requirements for critical infrastructure security indicators;
- risk control.

As noted above, critical infrastructure can be viewed as a set of objects/systems, including a subset of ICS $\{I\&C_q^i\}_Q$, which are connected to other subsystems by information links $I(t)_{inform}^{CI}(S_i \rightarrow S_j)$. The ICS is the point of integration of systems within the critical infrastructure, as it ensures the exchange of information and communication of risks. The security of critical infrastructures significantly depends on the vulnerability of these systems, which are always at risk of destructive impacts from the external environment, due to human actions or design defects in

hardware or software, technical failures, or unreliable, inaccurate, or insufficient data in the system's information resources.

As a rule, ICS has implemented security and protection measures with appropriate mechanisms and technologies to protect information from unauthorized access, cyberattacks and information leaks. There are tools for risk analysis, forecasting potential threats and identifying vulnerabilities in critical infrastructures, and it is necessary to work and modify security tools, solutions, and approaches on an ongoing basis, taking into account new threats and experience. It is required to ensure for the ICS of critical infrastructures functional resilience, a property that characterizes the ability of the system to maintain (automatically restore) the performance of a full or acceptable set of functions in the face of destructive influences [12]. This requirement is necessary because incidents in critical infrastructures and their information systems often occur unexpectedly, are difficult to predict and control, and therefore are almost impossible to prevent in full.

Modern approaches to protecting critical infrastructure facilities from cyber threats take into account this:

- the dynamic nature of the threat landscape; the constant emergence of new attack vectors and vulnerabilities, which leads to a generally predictive threat analysis;
- capabilities of artificial intelligence technologies, blockchain, machine learning, etc. for use in detecting security breaches and preventing cyberattacks;
- the specifics of a particular sector of critical infrastructure facilities and the relevant needs that affect cyber defense strategies, their flexibility and complexity;
- the need to implement international standards and regulations, cybersecurity and protection rules for critical infrastructures and their components.

Cybersecurity must constantly evolve as the number and complexity of cyber threats are constantly increasing. The application of modern cybersecurity practices for information systems and critical infrastructure facilities will significantly complicate the possibility of disrupting the functioning of critical infrastructures, leakage, distortion and unauthorized use of information on critical infrastructure facilities, and, accordingly, will reduce the number of incidents with catastrophic consequences and prevent the development of cascading accidents.

7. Conclusions

In critical infrastructures and their components, incidents often occur unexpectedly, and it is almost impossible to predict, control and prevent them in full, but ensuring the functional resilience of ICS and the use of cybersecurity practices will significantly increase the resilience of critical infrastructures and complicate the possibility of disrupting their functioning. The results of fundamental science (models for predicting risks of various nature, including unlikely ones, methods for assessing losses from the implementation of threats, etc.), engineering experience gained in close cooperation with "white" hackers, mechanisms for timely and adaptive response to incidents, restoration of functioning, and measures to counter threats will allow for a significant qualitative transition to more reliable cyber defense systems for critical infrastructure systems.

8. Acknowledgements

The authors are grateful to colleagues who took part in discussions on research materials at scientific and scientific-technical seminars and conferences.

References

- [1] "In 2022, the number of cyberattacks on Ukraine almost tripled. 90% of hacker groups from Russia are controlled by security forces" URL: <https://forbes.ua/news/v-2022-rotsi-kilkist-kiberatak-na-ukrainu-zroslo-mayzhe-vtrichi-90-khakerskikh-grup-z-rf-kontrolyuyut-siloviki-04052023-13454>
- [2] "Attacks targeting critical infrastructure are evolving" URL: <https://softprom.com/ua/ataki-natsileni-na-kritichnu-infrastrukturu-evolyutsionuyut>

- [3] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC <https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A32022L2557&qid=1686557595058>
- [4] "The Future of Cybersecurity: What Will it Be in 10 Years?" URL: <https://10guards.com/ua/blog/2021/11/09/the-future-of-cybersecurity-what-will-it-be-in-10-years/>
- [5] URL: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Oil_and_Gas/Pipeline/SecurityReference/SecurityIRD.pdf
- [6] Cyber-related process hazard analysis. URL: <https://www.isa.org/templates/news-detail.aspx?id=160155>
- [7] Cyber Process Hazards Analysis (PHA) to Assess ICS Cybersecurity Risk. URL: <https://youtu.be/8oZGYcRDjzc>
- [8] Quick Start Guide: An Overview of the ISA/IEC 62443 Standards. URL: <https://gca.isa.org/blog/download-the-new-guide-to-the-isa/iec-62443-cybersecurity-standards>.
- [9] Eugene Brezhnev, Vyacheslav Kharchenko, Viacheslav Manulik, Konstantin Leontiev Critical energy infrastructure safety assurance strategies considering emergent interaction risk. *Advances in Dependability Engineering of Complex Systems: Proceedings of the Twelfth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX*, July 2-6, 2017, Brunów, Poland.- Springer International Publishing, 2018, pp.67-78.
- [10] Kharchenko,V.S., Yakovlev,S.V., Gorbachyk,O.S. ,etal.: Provision of Functional Safety of CEUR Workshop Proceeding (ISSN 1613-0073). Vol.2318, p.64-76, (2018) [http://ceur-ws.org/Vol-2318//Critical Information-control Systems](http://ceur-ws.org/Vol-2318//Critical%20Information-control%20Systems). Kharkov: Konstanta, 272 p. Ukr. (2019).
- [11] "The number of cyber incidents registered in Ukraine in 2023 increased by 62.5%, - the State Special Communications Service" URL: <https://ms.detector.media/internet/post/33956/2024-01-12-killist-zareiestrovanykh-v-ukraini-kiberintsydentiv-u-2023-rotsi-zroslo-na-625-derzhspetsvvyazku>
- [12] Oleksandr Dodonov, Olena Gorbachyk, Maryna Kuznietsova Automated Organizational Management Systems of Critical Infrastructure: Security and Functional Stability // *Selected Papers of the XXI International Scientific and Practical Conference "Information Technologies and Security" (ITS 2021)*. CEUR Workshop Proceedings (ceur-ws.org). - Vol-3241 ISSN 1613-0073. URL: <http://ceur-ws.org/Vol-3241/p.1-12>.