Automated Organizational Management Systems of Critical Infrastructure: Security and Functional Stability

Oleksandr Dodonov[1], Olena Gorbachyk[1], Maryna Kuznietsova[1]

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

Abstract

An approach to improving the security of critical infrastructure based on the theory of survivability of systems is proposed. Taking into account the peculiarities of the functioning of automated organizational management systems (OMS), in the event of the emergence and implementation of emergencies, the possibility of ensuring the functional stability of these systems through the use of mechanisms of increasing survivability is justified. The concept of functional stability of OMS and methods of its estimation are defined. A formalized description and a qualitative resource model for assessing the limits of functional stability of automated OMS are proposed. The main tasks of the OMS in the process of developing management decisions in emergency situations are formulated. The creation and implementation of the analytical component of the automated OMS in order to improve the quality of management in the face of adverse effects and emergencies is proposed. It has been shown that special attention needs to be paid to the analysis and modeling of chains of influence that cross several sectors of critical infrastructure and can cause potentially unpredictable effects. The main problematic issues for modeling are formulated, the types of scenarios for emergency analysis are proposed, the tasks of creating and using resources of the analytical component of OMS for modeling situations, development of management decisions and analysis of their effectiveness are formulated. Typical approaches to ensuring the functional stability of automated OMS are analyzed: use of resource redundancy, special means of protection, organization of planned recovery procedures, application of sustainable structural solutions, construction of alternatives for communication networks and information exchange based on self-organizing systems. It is determined that the main modern requirements for automated OMS are the construction of a flexible structure of management of facilities and processes with the possibility of reorganization according to the requirements of external and internal environments, with the use of adaptation mechanisms that allow automated OMS to evolve along with the evolution of the operating environment, management facilities and in the case of a smooth emergency scenario. It is shown that in the conditions of rapid development of emergencies the functional stability of OMS can be supported by such mechanisms of increasing survivability as dynamic reconfiguration, recovery, compensation, counteraction to adverse effects.

Keywords

Organizational management systems, critical infrastructure objects, emergencies, functional stability, survivability, safety and security

1. Introduction

Automated Organizational Management Systems (OMS) of Critical Infrastructure Objects (CIO) are complex socio-technical systems that operate in a changing environment. Disorders in the

XXI International Scientific and Practical Conference "Information Technologies and Security" (ITS-2021), December 9, 2021, Kyiv, Ukraine

EMAIL: ipri2020@ukr.net (O. Dodonov); bges@ukr.net (O. Gorbachyk); marglekuz@gmail.com (M. Kuznietsova)
ORCID: 0000-0001-7569-9360 (O. Dodonov); 0000-0001-8492-4478 (O. Gorbachyk); 0000-0001-6054-418X (M. Kuznietsova)

© 2021 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

CEUR-WS.org/Vol-3241/paper1.pdf

functioning of the CIO (nuclear energy, chemical industry, military and aviation industries, transport, etc.) pose a potential threat to human life and the environment. Probability of emergencies at facilities, objects and critical processes infrastructures forces us to consider existence of such situations, to estimate risks of their realization. It is necessary to correctly determine the goals and required level of security of critical systems and infrastructures, to be able to predict possible losses in case of emergencies, to be able to prevent the development of dangerous conditions at infrastructure, to plan and implement restoration or "safe shutdown". Automated OMS should not only guarantee the proper functioning of the CIO in the specified operating conditions, but also to ensure an adequate response to a potential emergency, to initiate the implementation of appropriate measures to overcome it. There are problems that are not inherent in the normal mode of operation of the OMS and its components, the burden on managers is growing, the managers must make decisions in the face of adverse effects and limited time. To ensure the manageability of the CIO and critical infrastructure in general, the functional stability of the OMS is required to perform those functions which will allow to achieve the desired goal of functioning and to resist the destructive influences. Protecting critical infrastructure and increasing its resilience is one of the highest security priorities. In our research we will extend the application of this approach on new obtained data for the next years and will study in time the efficiency of SMART-characteristics time series analysis and how we can use their change for prediction the disk failure.

2. Automated Organizational Management System of Critical Infrastructure

Critical objects, or critical infrastructure objects, are identified in the [1] as the object's disruption (or cessation) of operation which may lead to loss of control, destruction of infrastructure, irreversible negative change (or destruction) of the economy of the country, entity or administrative-territorial unit, significant deterioration of the safety of the people, living in these areas. In fact, CIO are complex multi-level hierarchical systems, control of their state condition and functioning is performed by appropriate multilevel control systems using the means of automatic control and management according to certain technical regulations [2].

Automated organizational management systems are complex socio-technical systems where the collecting, analyzing and processing information about the object of management, its internal environment and interaction with the external environment is done [2]. There is always a risk of destructive effects on real systems from the environment, due to personnel actions or structural defects in hardware or software, failures of technical means, due to inaccuracy or insufficiency of data in the information resources of the system, which may lead to the inability to perform the required functions with a given level of characteristics [3]. Preservation (automatic recovery) of the ability to perform a complete or acceptable set of system functions in conditions of destructive (undesirable) effects is ensured by the functional stability of the system, which allows the user to trust the services of the system [3].

2.1. Functional Stability of Automated Organizational Management System and its Importance for Safety

The functional stability of the automated OMS means the property of the system to maintain the management structure and perform basic management functions within the limits set by regulatory requirements, in the presence of destructive (undesirable) effects. Due to the functional stability of the OMS is within the allowable space of states, that is, in addition to the fact that the system performs the main functions of its intended purpose, it does not have a negative impact on the environment and does not pose a threat to its existence [4].

Changes in the operating environment and in the critical infrastructure, the action of destructive factors of different nature can cause structural and functional disorders in the OMS, which can cause disruptions in its operation, the emergence of uncontrolled processes that can lead to the emergence and development of emergencies on the CIO, and even lead to disasters [5,6].

The range of threats to critical infrastructure in Ukraine is determined by the peculiarities of the security situation in the country. Fighting on the territory of Ukraine, high depreciation of fixed assets, serious problems with environmental and man-made safety dramatically increase the risk of accidents at high risk: power facilities, chemical and metallurgical enterprises and life support networks, both as a result of their intentional or accidental damage or loss of control over technological processes, and as a result of terrorist acts and sabotage [1].

Such a property as functional stability allows the system to ensure the performance of a certain critical range of functions in case of failure, failures or disturbances in the functioning of certain elements of the system due to destructive influences, both external and internal, to choose the appropriate mode of operation, using their own internal resources or obtained from outside, changing the structure, set of functions and operation of separate subsystems. The critical scope of management functions, as well as the allowable space of the OMS states, are determined based on the requirements to prevent unacceptable negative changes in the critical infrastructure [5]. Due to large-scale automation and informatization of management and technological processes, modern automated OMS are focused on working with information and intensive data exchange in the actual merger of automated production, production technologies with minimal human intervention in technological and management processes performed under normal operating conditions. Automated OMS usually implement certain standardized tools for assessing the situation on the CIO, tools for forecasting the development of events to prepare management decisions during the emergence and development of situations that disrupt the normal functioning of the CIO and OMS. Depending on the field of implementation, different indicators are used in scientific publications [4-9] to assess the functional stability of automated OMS, in particular, the amount of managerial functions performed, functions' performance indicators, the total weight of management functions performed, degree of controllability of technological processes, coherence of the management structure, parameters of analytical models for assessing functional stability, etc. The choice of indicators of functional stability should be made at the stage of design or automation of the OMS, taking into account the characteristics of critical infrastructure and its individual facilities, existing management structure, rules of subordination and information exchange in the social component of the OMS, set of critical management functions and time constraints on the safe termination of the CIO.

2.2. Definition and Formalization of the Concept of Functional Stability of Automated Organizational Management System

The operation of the automated OMS is aimed at resolving specific situations by implementing the overall process of the control system and the actions of the control object. If the situations that require management decisions are repeated and routine, then the automated OMS for their processing provide appropriate procedures and solutions that are typical and programmed. If there is a situation for which there are no proven programmed management decisions, than o make a really effective (purposeful, timely, comprehensive, etc.) decision it is necessary to form a sufficiently complete set of its possible alternatives and to choose from them the one that can be implemented with available resources (funds, stocks, opportunities).

An automated OMS (AOMS), as a socio-technical system, has the following resources at its disposal:

- hardware and technical - technical means that are part of the AOMS;
- software - software components of AOMS;
- information - information created and/or discovered, registered, evaluated with certain (specified) laws of degradation and renewal;
- social - officials and staff who implement information technology to perform the functions assigned to the AOMS.

If at a time interval Δt with any set of destructive influences $R_{\Delta t}$ there is at least one efficient distribution of AOMS resources, which will ensure the implementation of functions set in the current state of communication $F = \{\mathrm{f_n}\}$ with a quality level not lower $\mathrm{a}_{\lim}$, then AOMS is functionally stable over time interval Δt, that is

$$\forall(R_{\Delta t} \in R\ ,\ \mu_m^N \in M_{\Delta t}^N,\ \mu_m^G \in M_{\Delta t}^G),\ \exists k^*(Z_{\Delta t}) \in \mathrm{K},\ <\ k^*,\ \mu_m^N,\ \mu_m^G > \Rightarrow \mathrm{a}_{k*} \succeq \mathrm{a}_{\mathrm{lim}},$$

where $R_{\Delta t}$ – a subset of destructive influences that affect the system over time interval Δt from a set R of all destructive influences which can operate on AOMS;
$M_{\Delta t}^N = \{\mu_m^N\}$ – subset of quality indicators of spatial-temporal identification of CIO in AOMS on the basis of CIO monitoring data on time interval Δt, which is formed from an ordered set M^N indicators of the quality of spatial and temporal identification of COI in the AOMS, taking into account the data of current monitoring, computer models of CIO and the current destructive effects $R_{\Delta t}$;
$M_{\Delta t}^G = \{\mu_m^G\}$ – a subset of indicators of the quality of information exchange in the AOMS in the time interval Δt, which is formed from an ordered finite set M^G of indicators of the quality of information exchange in the AOMS, taking into account the current destructive effects $R_{\Delta t}$, available lines of communication over time interval Δt;
$Z_{\Delta t}$– a subset of resources (hardware, software, information, human) that are available for use in AOMS under destructive influences $R_{\Delta t}$ over time interval Δt from the set $Z = \{z_i\}$ of resources of AOMS, operating in normal conditions;
$K=\{k_l\},\ k_l=<Z_l^1, Z_l^2,..., Z_l^N>,\ Z_l^i \subset Z$ – set of resource allocations AOMS by N functions of the set of functions $F = \{\mathrm{f_n}\}$, which implement the requirements for functionality;
a_{k*} – vector of indicators of quality of realization of a set of functions $F = \{\mathrm{f_n}\}$ of AOMS when allocating resources in it and current indicators of the quality of spatial and temporal identification of CIO in AOMS μ_m^N and information exchange μ_m^G in AOMS, based on its spatio-temporal configuration over time interval Δt;
$\mathrm{a}_{\mathrm{lim}}$ – the limit indicator of the quality of implementation of a set of functions $F = \{\mathrm{f_n}\}$ AOMS, below which the functioning of the AOMS does not meet the requirements of the appointment.

Each vector a_i is a set $\langle q_{i_1}^1, q_{i_2}^2, ..., q_{i_N}^N \rangle$ of length N (where N – the number of management functions implemented in accordance with the purpose of the AOMS), and each element q_i^j reflects a certain level of quality of implementation of the j-function and belongs to the set Q^j, which, n turn, reflects a partially ordered finite set of possible levels of implementation quality of the j-function $Q^j = \{q_1^j, q_2^j, ..., q_{L_j}^j\}$.

For a set of functions $F = \{\mathrm{f_n}\}$, which are implemented by AOMS, there is a set Q levels of quality of functioning of AOMS, which consists of subsets that do not intersect, $\{Q^1, Q^2, ..., Q^N\}$, with elements $q_i^j \in Q^j$, $j = \overline{1, N}$, arranged according to the condition

$$q_1^j \le q_2^j \le ... \le q_{L_j}^j,\ j = \overline{1, N},$$

where q_i^j – the minimum level of implementation quality of j-function, corresponding to non-performance of the function, $q_{L_j}^j$ – the maximum level of quality with which AOMS can theoretically implement j-function, L_j – the number of gradations of the level of performance quality of the j-function.

The set Q is partially ordered, it is convenient to present in the form of a quasi-matrix of N - order with terms that are ordered sets Q^j [3]

$$Q = \begin{Vmatrix} q_1^1 & \cdots & q_{L_i}^1 \\ \vdots & \ddots & \vdots \\ q_1^N & \cdots & q_{L_N}^N \end{Vmatrix} = \left\| q_j^i \right\|, \; i = \overline{1,N}, \; j = \overline{1,L_i}$$

A set of vectors of quality levels $A = \{a_i\}$ of implementation of a set of functions $F = \{f_n\}$ AOMS also is partially ordered, moreover for any two vectors a_i and a_j, the vector a_i is better than a_j, if for each task f_m from a set of functions F the level of quality of its implementation q_i^m , belonging to the vector a_i, not worse than the level of quality of implementation of this function q_j^m , belonging to the vector a_j:

$$a_i \succeq a_j : \forall\, (\, q_{k_l}^l \in a_i,\; q_{m_l}^l \in a_j,\; l = \overline{1,N}\,)\,(k_l \geq m_l).$$

On the set A we introduce a metric: the distance between two vectors from this set is equal to the minimum difference between the indices of the quality levels of the implementation of each function of the set F , which are elements of these vectors

$$\forall(\, a_i, a_j \in A, a_i \succeq a_j\,)\; s\,(\, a_i, a_j\,) = \min_l\,(k_l - m_l),\; q_{k_l}^l \in a_i,\; q_{m_l}^l \in a_j,\; l = \overline{1,N}.$$

$a_{\lim}$ determines the limit of AOMS' functional stability to destructive influences from the set R , and the distance $s\,(\, a_{\lim}, a\,(k^*))$ can be interpreted as a margin of functional stability AOMS in the allocation of resources k^* . Changing requirements to the limit of functional stability $a_{\lim}$, you can solve problems to build reliable, survivable and safe (secure) systems.

For reliable systems $a_{\lim} = a^{relay}{}_{\lim}$ and accordingly:

$$\forall(R_{\Delta t} \in R\;,\; \mu_m^N \in M_{\Delta t}^N,\; \mu_m^G \in M_{\Delta t}^G),\; \exists k^*(Z_{\Delta t}) \in \mathrm{K}, <\, k^*,\; \mu_m^N,\; \mu_m^G > \Rightarrow a_{k*} \succeq a^{relay}{}_{\lim}\,,$$

where $a^{relay}{}_{\lim}$ is the minimum level of quality of implementation of functions F , in which the AOMS retains in time within the established limits the values of all parameters that determine its ability to perform functions F under certain modes and operating conditions.

For survivable systems $a_{\lim} = a^{surv}{}_{\lim}$,

$$\forall(R_{\Delta t} \in R\;,\; \mu_m^N \in M_{\Delta t}^N,\; \mu_m^G \in M_{\Delta t}^G),\; \exists k^*(Z_{\Delta t}) \in \mathrm{K}, <\, k^*,\; \mu_m^N,\; \mu_m^G > \Rightarrow a_{k*} \succeq a^{surv}{}_{\lim}\,,$$

where $a^{surv}{}_{\lim}$ is the minimum level of quality of implementation of functions F , in which the AOMS retains the ability to perform critical functions $F^{\kappa p} \subset F$ under conditions of destructive influences.

For safe (secure) systems $a_{\lim} = a^{safe}{}_{\lim}$,

$$\forall(R_{\Delta t} \in R\;,\; \mu_m^N \in M_{\Delta t}^N,\; \mu_m^G \in M_{\Delta t}^G),\; \exists k^*(Z_{\Delta t}) \in \mathrm{K}, <\, k^*,\; \mu_m^N,\; \mu_m^G > \Rightarrow a_{k*} \succeq a^{safe}{}_{\lim}\,.$$

where $a^{safe}{}_{\lim}$ is the minimum level of quality of implementation of functions F, in which the functioning of the AOMS does not pose a threat to human life and the environment.

If you can determine the level a_{τ} of the quality of AOMS functions from the set F at the current time τ and the maximum possible level $a_{\max}$ of quality of performing functions AOMS is known, than distance between vectors a_{τ} and $a_{\max}$ will determine the margins of stability in terms of reliability, survivability and safety.

The flow of destructive influences of different nature can cause failures in AOMS, and this will lead to changes in the vector, which will mean a decrease in reserves of stability or complete loss of diversion property of AOMS. In the case of recovery procedures based on the mechanisms of reconfiguration and / or reorganization of resources, or by introducing additional resources from the outside, you can restore the lost property. If the use of mechanisms of reconfiguration, reorganization in the AOMS allows to achieve compliance: $a^{relay}{}_{\lim} \succeq a_{\tau} \succeq a_{\max}$, then restored such a property as reliability; if $a^{surv}{}_{\lim} \succeq a_{\tau} \succeq a_{\max}$, then the system has survivability; provided $a^{relay}{}_{\lim} \succeq a_{\tau} \succeq a_{\max}$, the system becomes secure. The process of ensuring the functional stability of AOMS can be considered as a process of maintaining the current quality vector of AOMS functions at certain intervals in a given period of time by activating special tools and mechanisms for reconfiguration and reorganization of system resources.

3. Safety of Critical Infrastructure Objects in the Conditions of Destructive Factors and Development of an Emergency Situation

Security and protection of critical infrastructure involves, above all, ensuring the smooth and sustainable operation of critical infrastructure in certain modes, and the ability to prevent the destruction or irreparable damage, the cessation or loss of control of critical infrastructure objects due to all factors, and to ensure the rapid restoration of their operation if it is interrupted. The main task of protecting critical infrastructure is to prevent crises related to the functioning of critical infrastructure.

In [1] the following categories of threats are proposed, for which the protection of critical infrastructure should be configured:

1) *accidents and technical failures,* in particular, aviation accidents, nuclear accidents, fires, accidents in energy supply systems, emissions of hazardous substances, system failures, accidents and emergencies due to negligence, organizational errors, etc.;

2) *dangerous natural phenomena,* in particular, extreme weather conditions, forest, steppe and peat fires, seismic phenomena, epidemics and pandemics, space phenomena, hurricanes, tornadoes, earthquakes, tsunamis, floods, etc.;

3) *malicious actions,* in particular, the malicious actions of groups or individuals, such as terrorists, criminals and saboteurs, as well as hostilities in wartime.

Combined threats and threats are particularly dangerous, the implementation of which can lead to catastrophic and diverse cascading effects due to the interdependence of critical infrastructure elements.

Measures to counter threats to critical infrastructure are determined by the following guidelines [1]:

- *physical protection* – aimed at ensuring the protection of objects from unauthorized access, prevention and cessation of sabotage, theft or any other illegal seizure of equipment, devices and materials;
- *technical protection* – increasing fault tolerance and survivability of systems, functional redundancy;
- *staff* – training and testing of personnel, control of their ability to perform certain functions, security of personnel;

- *Information Technology* – protection of information, communication systems and management;
- *legal* – settlement of issues of personnel response and functioning of infrastructure in crisis situations, consolidation of division of responsibilities in normative and legal documents, development of manuals and instructions for personnel, including on interaction in crisis situations;
- *recovery plans* – creation of plans, reserves and services for quick recovery of lost functions.

The following modes of operation are defined for the system of protection of critical infrastructure, which is a part of the automated OMS CIO:

- crisis prevention;
- crisis management;
- operation in a state of emergency;
- functioning in martial law.

The normal mode of operation of critical infrastructure for the protection system is a regime of monitoring and risk assessment of crisis situations, in which continuous crisis prevention should be provided.

In the event of a crisis, the critical infrastructure protection system should switch to crisis management. If a crisis situation occurs in a particular sector of critical infrastructure, then due to the interconnectedness of sectors (interconnections / impacts of facilities from different sectors), it can spread to all critical infrastructure and lead to the most serious consequences for the country.

Crisis management regime provides for the involvement of emergency measures to contain factors, improve the conditions and characteristics of the security environment, or improve the functioning of certain objects of critical infrastructure, etc. The same regime is used in the restoration of critical infrastructure after malicious actions, accidents and failures, significant impact of dangerous natural phenomena. The transition to the operation of the OMS in states of emergency and martial law should take place in the event of the proclamation of appropriate legal regimes in the event of an emergency, terrorist threat or armed invasion.

3.1. The Functions and Tasks of Automated Organizational Management System in case of Threat or Emergency

An emergency (crisis) situation is a violation of normal living conditions and activities of people on the site or territory, caused by an accident, catastrophe, natural disaster, epidemic, fire, use of means of destruction [1]. There are 5 typical stages (phases) of emergency development (emergency): the accumulation of deviations - the initiation of an emergency - the manifestation of the main impact factors - the action of secondary impact factors - the action of residual impact factors. It is necessary to prevent the emergence of critical infrastructure by all possible means, to adequately respond to emergencies and to have the means to eliminate the consequences of emergencies.

Occurrence and development of emergencies occurs in real time, so the solution of problems of monitoring and analysis of stages of emergencies must also take place in real time, which requires spatial and temporal identification of CIO and infrastructure as a whole. Emergency management systems must take into account the nature and speed of emergency development, control not only the parameters of the CIO, but also the characteristics of the environment. The following functions must be performed in the automated OMS:

- monitoring, the main task of which is the continuous processing of data from the CIO in real time and signaling the departure of certain parameters beyond acceptable limits;
- diagnostics of the place of occurrence of the emergency to localize the area of malfunctions or errors;
- forecasting the consequences of certain events or phenomena based on the analysis of monitoring data from various sources;
- planning actions to prevent the development and spread of emergencies;
- correction of management decisions in case of diagnosing errors and failures;
- ensuring the management of the CIO and the relevant mode of operation of the OMS itself;
- providing the necessary information and recommendations to all levels of government.

In the conditions of emergency situations in the functioning of the AOMS there are problems associated with the high rate of changes in the parameters and state of CIO, unpredictability of events, dependence of information flows on the situation and communication system, changing the distribution of functions, expanding or narrowing the scope, etc. [4]. In such conditions, it is desirable to have the means to support the development of management decisions, in particular, to have pre-established schemes of action in the development of emergencies, to have a base of precedents, systematized and accumulated experience in overcoming previous emergencies.

Given the interpenetration and, inter alia, the interdependence of critical infrastructures, it is necessary to ensure that the AOMS performs the function of identifying, analyzing and modelling chains of influence that cross several sectors of critical infrastructure and lead to potentially unpredictable effects. For chains of influence, there are several types of interdependencies that make up the paths between infrastructure components (nodes) of the type: $a \to b \to c \to d \to ... \to y \to z$.

This path reflects (models) the cascading consequences of the event or the derived dependence of the node-object z on the node-object a, which is denoted ($a \Xi z$). A chain constructed in this way may not be the only one, and if the end effect is the effect on z of several object nodes, it is affected ($abc \Xi z$). Pathways are not unique in terms of effect, they may change over time, and their behavior may be cumulative in nature, that is, the end effect may be the culmination of several possible events. To analyze infrastructure interdependencies and forecast changes in infrastructure, it is necessary to determine:

1. What will be the cascading effect on the subset of object nodes {x, y, z, ...}, given the set of initiating events $\{P(a), P(b), ...\}$?

2. What will be the set of events $\{P(a), P(b), ...\}$, what can cause a cascading effect given the set of object nodes {x, y, z, ...} and the desired end state?

3. What will be the derivative of interdependence ($ab \Xi xyz$), based on the set of events $\{P(a), P(b), ...\}$ and the set of observed results on the nodes-objects {x, y, z, ...}?

4. What is the subset of critical nodes {x, y, z, ...} of all networks that will negatively affect a particular function through a direct or derivative relationship, given the set of infrastructure networks and the critical function?

Management decisions to ensure the security and protection of critical infrastructures depend on the answers to these questions. Some of the impacts and their consequences that can be predicted, it is advisable to analyze and prepare appropriate effective management decisions.

The AOMS should have the means to act in the "slow" and "fast" scenarios of emergency development. In a "slow" scenario, there is time to apply certain means of protection and perform certain protective actions to localize the emergency and prevent its further spread by the infrastructure. In the case of a "fast" scenario of development of the emergency, events in the infrastructure unfold rapidly. It is desirable to apply such measures and means that would allow to react before the destruction of the CIO and infrastructure.

The functional stability of the AOMS in the conditions of the "fast" scenario of emergency development becomes extremely important, because the strict time constraints require:

1) assess the parameters of the operating environment, taking into account safety risks and possible consequences of emergencies;

2) identify places in critical infrastructure that have the highest risks, and assess their impact on the structure and functioning of individual CIOs, predict potential losses;

3) to carry out spatio-temporal identification of CIOor to use available dynamic models for forecasting of a probable condition of infrastructure and CIO and to choose from possible variants of administrative decisions more rationally for reaction to current events;

4) determine and permanently monitor the parameters of the CIO, assess and forecast the state of the CIO, if possible, to build scenarios of events taking into account the current external and internal influences on the CIO and AOMS;

5) determine the list of necessary resources for counteracting emergencies, develop scenarios for localization and elimination of the consequences of emergencies.

After the elimination of emergencies, it is advisable to analyze the adopted and implemented management decisions, evaluate their effectiveness, although with the evolution and increasing complexity of CIO, its parameters and components change, which leads to an increase in the number and variety of kinds and types of risks and the entire infrastructure [2,8,9], so the analysis of the range of possible risks should be constantly monitored, the state of the selected parameters and the environment should be monitored, and new risk situations should be modelled [6,10-12].

4. The Survivability of the Automated Organizational Management System as a Factor in maintaining its Functional Stability

The development of information technology, automation of a number of management functions have led to a change in perceptions of the ideal OMS as a stable and fully manageable system with a rigid hierarchical structure. Requirements for modern OMS include the construction of a flexible structure of management of facilities and processes with the possibility of reorganization according to the requirements of external and internal environments, with effective mechanisms of adaptation, allowing OMS to evolve along with the evolution of the operating environment and management objects.

The complexity of the CIO, both technological and operational in nature, leads to an increase in the number of elements involved in the monitoring and management processes, diversification of interaction structures in OMS, which leads to an increase in the number and variety of kinds and types of risks, which can cause disruptions in the functioning of the CIO and in the infrastructure as a whole. It is impossible to predict and protect critical infrastructure from all risks, therefore, the safety of its operation should be ensured based on the conditions of "if, then". Such conditions require adequate quality management and functional stability of AOMS of the critical infrastructure .

To ensure the functional stability of AOMS in the design of its technical component, a certain redundancy is traditionally introduced (structural, software, time, resource); built-in control systems are being implemented; contours of protection of AOMS against destructive influences of external environment are formed; components with the increased level of protection and reliability are chosen. These traditional solutions have certain limitations. Additional redundancy, unfortunately, leads to a deterioration of the technical and economic characteristics of the systems. Monitoring systems observe a number of parameters, but may not always or not at all provide an adequate response to an abnormal situation and may not reduce the likelihood of such situations. The protection circuit can minimize the influence of external factors, but does not completely eliminate it. The choice of element base with the increased level of protection and reliability does not provide functional stability of system when failure has already occurred [4, 6-9].

Ensuring the functionality and security of computer systems, as part of AOMS, involves the implementation of a comprehensive security system using firewalls, anti-virus software, in-depth application traffic analysis procedures, identification and authentication of users, security incident management systems with the ability to track and manage incidents, etc. The use of information technology in AOMS to ensure effective management of the CIO in the emergence and development of emergencies, and today, in particular, in areas of hostilities, has led to new security requirements:

- formation and maintenance of a zone of continuous information coverage of a large plane;
- ensuring the scalability of the communication network in order to increase the coverage area and the density of information support;
- creation of wireless transport channels for communication of access points in the "one-to-one" mode;
- ensuring noise immunity, protection from imitation interference, increasing resistance to loss of individual network elements;
- guaranteeing the smooth operation and adaptability of the communication network.

Communication requirements are partially met by technology Mesh – construction of networks, a distinctive feature of which is self-organized architecture (Wireless Mesh Network (WMN), which are also called cellular networks [13]. Mesh networks are built as a set of clusters. The coverage area is divided into cluster zones, the number of which is theoretically unlimited. Mesh networks use special protocols that allow each access point to create network subscriber tables with traffic channel status monitoring and support for dynamic traffic routing along the optimal route between neighbouring points. If any of them fails, the traffic is automatically redirected to another route, which guarantees not just the delivery of traffic, but its delivery in the shortest time. Mesh technology is based on a decentralized network design scheme, and access points that operate on Mesh networks provide subscriber access services and act as routers / repeaters for other access points on the same network. This makes it possible to create a self-installing and self-healing segment of a broadband network. Using such a network allows you to quickly recover traffic in the event of failures or intentional damage to individual network nodes. The disadvantage of Mesh networks is the use of intermediate points for data transmission, which can cause delays in the transmission of information, and, consequently, reduce the quality of real-time traffic.

AOMS in the conditions of origin and development of the emergency system operates under constant variability of the external environment, uncertainty of external and internal destructive influences, the impossibility of clearly taking into account the reaction of the environment to the actions of the system and the response of the system to external influences, that is, in terms of the manifestation of such a fundamental systemic property as survivability. Due to this property, any system can be stored as a whole in the unpredictable, sometimes extreme, conditions, adapt to them, changing the behavior, structure or system-wide purpose of the operation. High survivability systems are characterized by flexibility in management, variability of operation algorithms, transitions from a hierarchical management model to linear, network, network-centric, and vice versa, which ensures the safe operation of the system itself and its achievement of the system-wide purpose of operation.

Low survivability systems break down quickly, and if there is a low survivability of AOMS critical infrastructures, it can lead to the development of cascading accidents with significant material losses [7], while AOMS, characterized by increased survivability, are destroyed gradually, retaining partial functionality, limited performance [6]. There is time to make decisions regarding the transition to a safe mode of operation, emergency stop, isolation of damage, preventing their spread, and so on.

Survivability is a fundamental intrinsic property of complex systems, regardless of the conditions of their operation, and it is manifested only in the presence of destructive effects, damage or even loss of system components and component failures [2,6].

In the event of an emergency, the functional stability of AOMS CIO can be supported (increased) by mechanisms to ensure survivability, after all, survivability is the property that allows the system to adapt to new operating conditions in the presence of destructive influences, maintain or promptly restore the functions of the system with minimal loss of efficiency in case of degradation or failure of individual components of the system through the use of available operational resources.

To maintain the functional stability of the AOMS, it is advisable to use the following mechanisms of survivability ensuring [6,14]:

- *recognition and localization* – to detect attacks on AOMS information components, successful intrusions into the system and its information resources, the occurrence of risks of loss or distortion of information, increased risk and failure of vital (critical) components of AOMS, identification of the failed element or component, fixing the output of certain parameters of AOMS, CIO and environment beyond the established limits;
- *counteraction* – creation and application of a set of predetermined means and measures to maintain the specified operating conditions and minimize losses associated with the transition to a non-standard mode of operation;
- *recovery and restoration* – development and use of a set of methods and software and hardware to restore the functionality and performance of components and the system as a whole, its information resources and information and communication tools under adverse effects;
- *adaptation* – development of a set of procedures for targeted changes in the parameters and structure of AOMS based on information about changes in operating conditions, the emergence of unforeseen situations, the consequences of violating the security of information resources;
- *reorganization* – development of algorithms and procedures for redistribution of failed component functions between operational components or, in case of impossibility of redistribution, - organization of system transition to a new purpose of operation;
- *reconfiguration* – performing automatic (automated) restructuring of the structure of the information exchange network or changing the algorithm of operation to achieve the greatest efficiency of the purpose of operation on the available operational resources of the system;
- *reconstruction* – application of reduction of the purpose of operation (list of AOMS functions performed) and system resources to certain base levels, when the system can perform only a clearly

defined set of functions, save a certain amount of information, ensure smooth degradation of certain parameters.

These mechanisms integrate the tools and design solutions implemented in the system to increase reliability and fault tolerance, monitoring, automatic control and compensation, built-in algorithms and means of protection of components and components of AOMS, etc.

5. Conclusions

In the context of hostilities in Ukraine, which lead to a significant large number of emergencies, effective management of critical infrastructure has become an extremely important task. The functioning of the automated organizational management system is aimed at resolving specific situations by implementing the overall process of the control system and the actions of the control object. Rapid response to emergencies at the objects of the critical infrastructure and in the infrastructure as a whole, localization of the emergency zone, preventing the development of cascading accidents, improving the level of protection and safety of critical infrastructure – here are the tasks that AOMS provides. The functional stability of automated organizational management system, as a property of the system to maintain the management structure and perform management functions within the limits set by regulatory requirements, in the presence of destructive influences – is an affecting on the safety of critical infrastructures factor. Improving the survivability of automated organizational management system of the objects of the critical infrastructure allows even in the "fast scenarios" of emergency development to reduce the negative consequences of emergencies, due to the validity and timeliness of management decisions, preventing the complete loss of of the critical infrastructure objects management.

The expediency and effectiveness of the proposed approach to ensuring the safety of the objects of the critical infrastructure and critical infrastructure in general in the presence of destructive influences by increasing the functional stability of automated organizational management systems were tested and demonstrated when creating the automated OMS of special purpose.

References

[1] Green Paper on Critical Infrastructure Protection in Ukraine. Kyiv, 2015. 35p. (in Ukrainian)

[2] Dodonov, O., Gorbachyk, O., Kuznietsova, M. Increasing the survivability of automated systems of organizational management as a way to security of critical infrastructures. In: XVIII International Scientific and Practical Conference «Information Technologies and Security» (ITS 2018), CEUR Workshop Proceeding (ISSN 1613-0073). 2018. Vol.2318. P.261-270. [Online]. Available: http://ceur-ws.org/Vol-2318/paper22.pdf.

[3] Korolev, A.N. Functional stability of navigation and information systems. // University news. Instrument making. 2018. T.61, №7. P.559-565. (in Russian)

[4] Emergency management systems. Available: http://risk.keldysh.ru/risk/g112.htm

[5] Barabash O.V., Durnyak B.V., Mashkov O.A. etc. Ensuring the functional stability of complex technical systems // Modeling and information technology: Coll. Science. works, 2012. - Kyiv: Institute of Modeling Problems in Energy named after G.Ye. Pukhov. National Academy of Sciences of Ukraine, B.64. Pp. 36–41. (in Ukrainian)

[6] Kharchenko, V.S., Yakovlev, S.V., Gorbachyk, O.S. , et al. Provision of Functional Safety of Critical Information-control Systems. Kharkov: Konstanta, 2019. 272 p. (in Ukrainian)

[7] Failure Mode, Effects & Criticality Analysis (FMECA). Available: https://quality-one.com/fmeca/

[8] N. Kuznietsova, M. Kuznietsova, Data mining methods application for increasing the data storage systems fault-tolerance, IEEE 2nd International Conference on System Analysis & Intelligent Computing (SAIC), 2020, pp. 315–318. Available: https://doi.org /10.1109/SAIC51296.2020.9239222

[9] Dodonov, O., Gorbachyk, O., Kuznietsova, M. Survivability of organizational management systems and the maintenance of critical infrastructure security. In: XIX International Scientific and Practical Conference «Information Technologies and Security» (ITS 2019), CEUR

Workshop Proceedings 2019, Vol.2577, pp.1-10. Available: http://ceur-ws.org/Vol-2577/paper1.pdf

[10] Boyarchuk, A., Brezhnev, E., et. al. Security of critical infrastructures: mathematical and engineering methods of analysis and provision, 2011. Kharkiv. 642p.

[11] Kharchenko, V., Kovalenko, A., Andrashov, A. Security of safety important I & C systems/ Standards and Standardization: Consepts, Methodologies, Tools and Application. 2015, pp.1279-1316.

[12] Kharchenko, V., et al. Critical infrastructures safety assessment combining fuzzy models and Bayesian belief network under uncertainties // Advances in intelligent systems and computing, 2013, vol. 224, pp. 245-254.

[13] Cilfone, A.; Davoli, L.; Belli, L.; Ferrari, G. Wireless Mesh Networking: An IoT-Oriented Perspective Survey on Relevant Technologies. *Future Internet* 2019, *11*, 99. Available: https://doi.org/10.3390/fi11040099. https://www.mdpi.com/1999-5903/11/4/99/htm .

[14] Oleksandr G. Dodonov, Olena S. Gorbachyk, Maryna G. Kuznietsova Dynamic Reconfiguration in Automated Organizational Management Systems// Selected Papers of the XX International Scientific and Practical Conference "Information Technologies and Security" (ITS 2020). CEUR Workshop Proceedings (ceur-ws.org). - Vol-2859 ISSN 1613-0073. URL: http://ceur-ws.org/Vol-2859/paper13.pdf.