DOI: 10.35681/1560-9189.2025.27.1.335694

UDC 004.7: 004.89

V. F. Grechaninov
Institute of mathematical machines and systems problems NAS of Ukraine
42, Academician Glushkov Avenue, 03187 Kyiv, Ukraine

On the need to use modern capabilities in situational management to protect the state's critical infrastructure

The article examines modern opportunities for improving situational management (SM) mechanisms in connection with the innovative development of situational centers (SCs). The requirements for SM are presented. The role of SCs in managerial activities, their structural organization, and possibilities for technological modernization are demonstrated. The article explores the potential use of artificial intelligence agents in SM systems. Scenario modeling method is described. Other methods that can be used to create and model scenarios for SM work to counter threats to critical infrastructure are listed. The need for their early development is presented. Situational management is described using the example of protecting the functioning of Ukraine's unified power system. The tasks and functions of cybersecurity in the electric power industry are highlighted, along with its existing shortcomings. The necessity of creating a unified network of SCs within executive authorities and administrations of critical infrastructure facilities is justified. This network would facilitate protection management and, in the event of destruction, ensure the rapid restoration of critical infrastructure facilities and their functions.

Key words: *situational management, artificial intelligence agents, situational centers, scenario-based approach, scenario modeling, cybersecurity, LLM (large language model).*

Relevance of the Topic

The modern era is characterized by-widespread use of electronic communications. Digital transformation is now an objective process that permeates all spheres of social existence. Ensuring the stable functioning of society's infrastructure is the responsibility of executive authorities, as well as the owners and operators of critical infrastructure facilities (CIFs) in each country.

Russia's war against Ukraine has clearly exposed new challenges to national security. The consequences of missile and drone strikes lead to accidents, disasters, and other emergencies. These incidents are becoming increasingly large-scale and dangerous

for people, economic stability, and the population's vital needs. Since the beginning of Russia's full-scale invasion, Ukraine's energy system has suffered continuous destruction, leaving thousands of homes, as well as industries and businesses, without electricity.

The disruption of infrastructure functionality has become a significant factor in undermining the stability of the socio-economic situation in our country. For three years now, we have been observing and experiencing Russia's deliberate actions aimed at severely impairing the infrastructure's ability to fulfill its functions. Therefore, the CIF protection system has a targeted focus, namely, to ensure that CIFs can carry out their designated tasks and functions. This, in turn, has led to an ongoing process of decision-making (situational management). These decisions are made by state-level leaders and policymakers, the military, CIF administrations, etc.

Problem Statement

Weapon strikes and cyberattacks by the Russian Federation on the CIF disrupt their functioning. This leads to problems with the provision of essential services to the population, economic losses, and human casualties.

Applied approaches do not sufficiently address the issue of CIF security, although responsibility for it is shared by many different stakeholders. As a rule, CIF operators focus on limited goals and specific events, and cannot reasonably determine which threats to them will emerge next and how to effectively protect the CIFs.

Some attempts to use individual innovations have not yet become the universal effective mechanism for improving situational management (SM) of CIF protection. The issues of implementing innovative capabilities of the SM are multifaceted. It is necessary to improve the existing CIF protection, including using modern capabilities of situational centers (SCs) and developing appropriate scenarios for management. For this purpose, the ideas of a scenario approach and the use of SC capabilities using artificial intelligence (AI) agents to improve the protection of CIF are considered.

Identification of the unexplored aspect of the overall problem

It cannot be claimed that there have been no conceptual ideas in this managerial activity. However, there are some contradictions between theoretical recommendations and practical actions to expand the use of scenario approach and AI capabilities in situational management for protection of CIF. Relevance of and problems related to the topic of the article require further research in this area. Information technologies are ready for transformational changes driven by rapid scientific and technological progress. They demand the integration of human and artificial intelligence to improve SM.

The aim of this article is to examine some modern opportunities and approaches for the development of SM for protection of CIFs using a network of SCs.

Presentation of the Main Material

It is essential that the basis of the critical infrastructure (CI) protection system be «preventive planning» and the capability to implement it. At various management levels, there must be an adequate assessment of the risks of crisis situation formation to prevent threats that could lead to the destruction of CIFs or impede their functionality

[1]. In the event of an impact, prompt and decisive actions should be taken to immediately restore the functions that sustain the Armed Forces and the life support of the population.

For this purpose, it is imperative to promptly implement modern decision-making technologies (described in this article) into operation of the situational centers' network, utilizing their databases and accumulated knowledge.

A management mechanism is a set of functions, methods, technologies, principles, and tools aimed at effective use of the resources of a situational management system to achieve its established goals.

Situational management is a type of management in which the following components are essential: forecasting potential dangers, analyzing measures to reduce negative consequences, eliminating them, and using the acquired experience to inform future decisions [2]. Decisions can be made based on knowledge, experience, intuition, expert guidance, modeling results, and other factors.

In order to improve SM in state authorities, the Decree of the President of Ukraine dated June 18, 2021 No. 260/2021 «On improving the network of situational centers and digital transformation of the sphere of national security and defense» set the task of expanding and further developing the network of SC, which should include the Main SC of Ukraine, the Government SC, SCs of central executive authorities, etc. [3].

The Model Regulation on the Situational Center of the Central Executive Body and the Regulation on the Situational Center of the Cabinet of Ministers of Ukraine were approved by the Resolution of the Cabinet of Ministers of Ukraine dated July 11, 2023 No. 705 [4]. However, this situational center has not yet been put into operation.

It is advisable to have a modeling complex (MC) in this center for a unified system of situational centers (USSC) involved in the management of the protection of the CIF. Some of the main tasks of the MC will be:

— development of technical solutions and special software for creation of automation systems for the USCC of government agencies and facilities included in the specified system;

— implementation of information exchange and operational information and analytical support for decision-making.

The capabilities of SCs should provide timely information about potential threats and assist in objectively assessing risks through methods such as simulation, cognitive, and geospatial modeling. Forecasting technologies should be employed to understand the real threats to CIFs and to ensure their protection.

Analysis of crisis management issues has allowed for the identification of certain state functions in this context that may be particularly relevant during the war with Russia. Above all, there is a need to monitor the interrelationships between the scale and potential rate of destruction of CIFs and the emergence of dangers that threaten the country and its social stability.

Ongoing technological progress necessitates innovations in SM, including implementation of novel approaches such as artificial intelligence (AI). Innovative development is based on structural reorganization and technological modernization of SCs. Its evolution can be characterized as a transformation process in situational management. It is known that decision theory has been the driving force behind the development of AI.

SM on an innovative basis requires solving a range of problems in related fields of activity of the entity in which it is implemented.

A SC is a modern system comprising a set of automation tools and software designed to perform tasks using SM methods. It can also be defined as a software-hardware complex intended to support the adoption and formulation of appropriate, necessary managerial decisions. A SC can operate in the following modes [5]:

— everyday operation;
— heightened readiness;
— response to an emergency situation;
— state of emergency.

We consider a SC as a management system that can integrate human and artificial intelligence, information technologies with the aim of protecting the functionality of CI. It is an instrument for organizing the information-analytical support of the managerial process, in which the management cycle is as follows:

— monitoring the state of protection of CIF functionality;
— identifying problems that require resolution;
— preliminary expert assessment (individual work by experts);
— situation modeling;
— expert evaluation regarding the forecasting of situation development (collective work by experts);
— decision making;
— task formulation.

For the purpose of utilizing the SC in SM, we view it as a hardware-software complex for collection, accumulation, and processing of information necessary for preparing and making decisions to ensure sustainable operation of the state's critical infrastructure system. Modern SCs, as automated information-analytical management systems, are designed to assess the potential development of events and to support decision-making (Fig. 1).

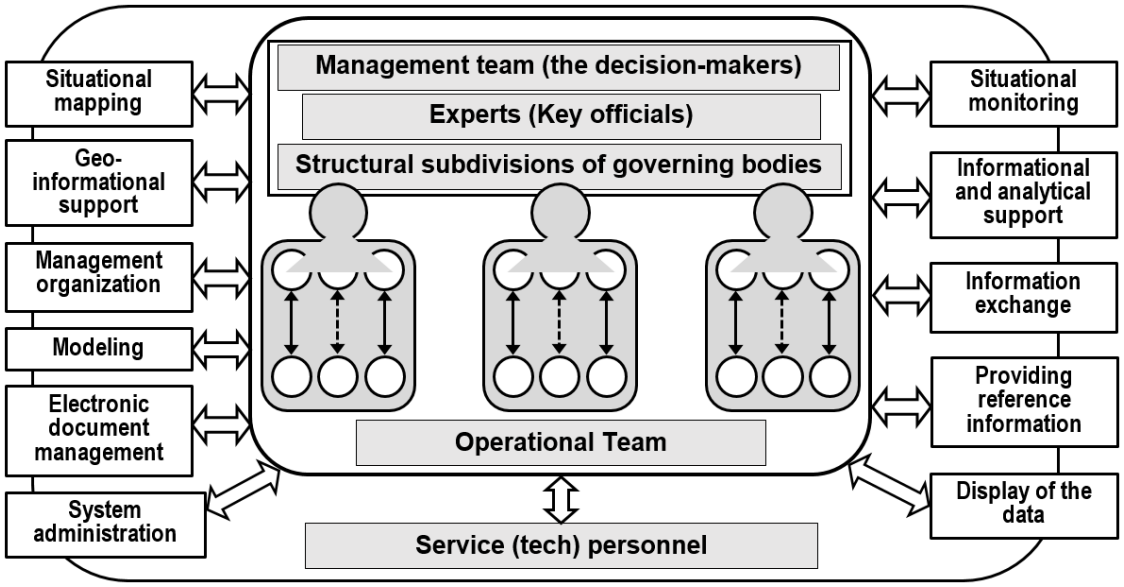

Fig. 1. Basic functions and typical organizational structure of situational centers of public authorities

SM process involves-three groups of participants:

1) decision-makers;

2) experts — specialists in their field who possess the information related to the problem;

3) analysts — experts in decision theory who develop various models (informational, mathematical, etc.).

Let us consider the possibility and necessity of using AI agents in SM systems. An AI agent is an intelligent system designed to perceive its environment, make decisions, and take actions with the aim of achieving a specific goal (Fig. 2).

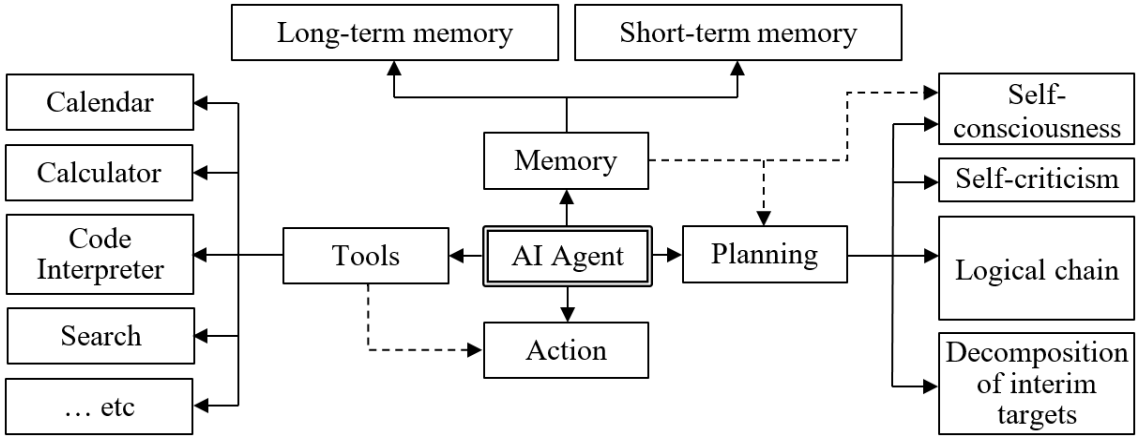

Fig. 2. Technical architecture of an AI Agent

AI agents represent a paradigm shift from traditional computing. They are not just tools we use but intelligent partners that can learn, adapt, and solve problems alongside us [6]. The concept of AI agents is not new, but recent technological advancements have transformed them from theoretical constructs into powerful practical applications.

Using advanced models, such as LLM (large language model) and other basic models, AI agents develop a deeper «understanding» of the context. In decision-making, AI agents can make trade-offs, predict outcomes, and prioritize actions.

On March 30, 2025, Deputy Prime Minister for Innovation, Development of Education, Science, and Technology — Minister of Digital Transformation of Ukraine Mykhailo Fedorov, speaking at the AI Day conference by Forbes Ukraine, entirely dedicated to the introduction of AI in Ukraine, announced that the development of a national LLM was starting. The launch of the national LLM will launch mass production of Ukrainian AI tools, which is a matter of national security. The LLM will allow data processing within the country, which is strategically important for the use of AI in defense, government organizations, etc. The launch of the LLM is scheduled for November-December 2025. AI products for the state and the defense sector will be implemented on the basis of the national LLM [7].

Currently, Chinese scientists have already introduced a new AI agent, Manus, capable of solving incredibly complex tasks. Manus positions itself as «AI that turns thoughts into specific actions». This agent not only analyzes information; it can also in-

dependently interact with its environment — from searching the internet to performing real-world tasks.

Creators of Manus claim that their agent can handle a wide range of tasks. For example, it can build a website from scratch, organize a trip to Japan, assess the investment prospects of Tesla stocks, or even create an interactive course for teachers. Experts believe that such agents could drive a true revolution in AI development.

Manus operates within a multi-agent system, where it acts as a coordinator, distributing tasks among specialized agents [8].

Autonomous multi-agent systems (Fig. 3) involve AI agents collaborating as interconnected networks, jointly solving complex problems not only in situational management systems but also in such areas as decentralized systems management, supply chain optimization, drone swarm control, etc.

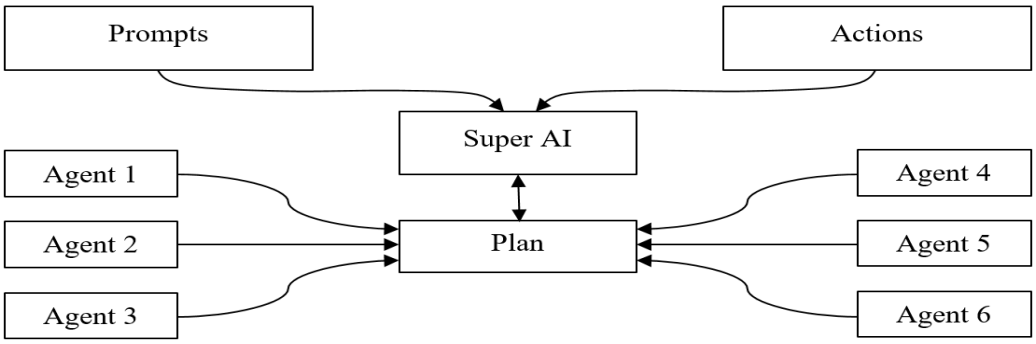

Fig. 3. Multi-agent cooperation chart

Using machine learning algorithms to analyze large amounts of data from multiple sources can help predict potential threats before they materialize.

A key advancement in situational awareness is integration with on-premises AI video analytics tools (which does not require access to the cloud). This technology processes and analyzes video data directly on the device where it is recorded, significantly reducing latency and bandwidth usage. AI situational awareness technology can be applied to instantly identify and classify CI threats. This allows for immediate decision-making and real-time response.

It is known that decision making is based on appropriate knowledge. Knowledge is formed through accumulation and analysis of information. Current situation within SM increasingly requires-deeper investigation of accumulated data through construction and modeling of scenarios.

Within SM, the scenario method has gained wide popularity as it allows for description of the most likely course of events and probable consequences of decisions made. There is a significant difference between the scenario approach and traditional planning. A scenario can be constructed at any hierarchical level of management.

Scenario of analytical activity is a certain sequence of actions for solving assigned problems by describing predicted or possible course of events in a particular field related to the activity of the object.

Principles of scenario modeling are well-known [9, 10]. In our view, the main task of a scenario is to provide the key to understanding of the problem.

Scenario development is a relatively lengthy and creative stage of scenario analysis. A wide range of methods are employed in scenario development: simulation and mathematical modeling, situational analysis, idea generation techniques, expert methods, and so on. These methods provide the basis for constructing, using modeling, various scenarios of information systems operation. Scenario modeling should be an adequate method of a scientifically based approach to studying the problem of forecastting the development of various processes [11]. It is an appropriate method for researching the prospects of innovative process development using a methodology based on scenario modeling algorithm.

A brief description of the scenario modeling technology is as follows:

— preparation of the scenario for modeling;

— transferring the task formulation to functional subsystems for implementation of the scenario;

— simulation of the situation on computers;

— monitoring the scenario's operation;

— implementation of modeling algorithms and presentation of the results;

— analysis of the modeling results.

The number of modeling processes and their representation will depend on the purpose of the modeling. Scenario analysis provides a set of detailed descriptions of the sequence of events which, with a forecasted probability, may lead to desired outcomes based on the variants of development considered by the scenario planner.

Studying the real situation being modeled may take quite a time. Therefore, the best conditions for developing a scenario to protect the sustainable operation of CI in the country are found during the everyday operation of the SC. In such a mode, there is sufficient time to answer the questions: what to protect; from what to protect; with what means to protect; and what the protection outcomes should be. During execution of these actions, data collected and accumulated in the respective SC databases will be used.

When time permits, it is advisable to use the scenario approach in modeling the process of analytical activity to meet information needs and support the decision-making of the responsible official (Fig. 4).

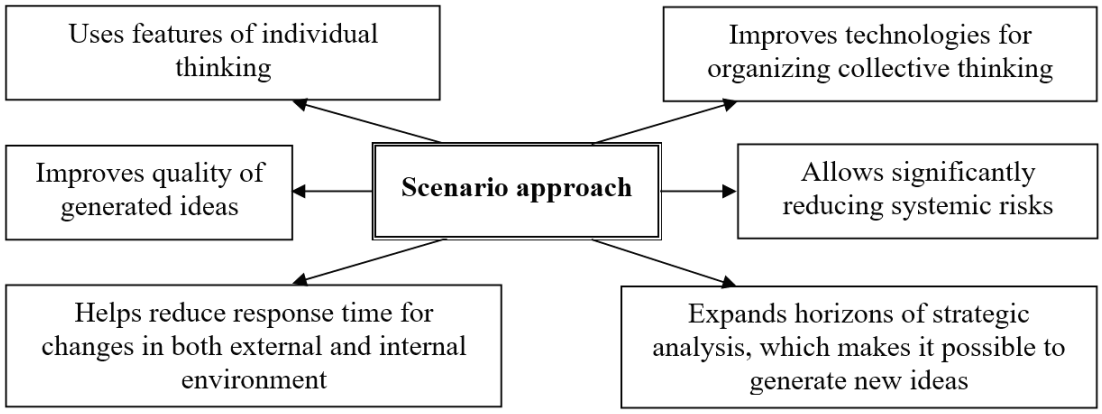

Fig. 4. Advantages of applying the scenario approach for development of SM

If the scenario is developed in advance and the SC database is filled in a timely manner with information regarding the necessary data and where it is needed, how to deliver it, install it, etc., depending on the field of activity of the CIF, then the SC has the opportunity to develop a security management model for sustainable functioning of the CIF, and a model for rapid and effective restoration of the CIF functioning in the event of its disruption.

It is possible to simulate counteraction to identified threats. As a result of simulations, we can obtain an assessment of the effectiveness of counteraction and make adjustments to defense systems taking this assessment into account. Then we have a better opportunity to determine the forces and means necessary to counter threats and formulate requirements for them. It is also possible to determine the necessary material and technical resources.

Let's consider a scenario for countering CI threats. To develop a scenario of possible events and make appropriate decisions for protection management, it is necessary to:

— conduct a comprehensive analysis of the assets requiring protection, as well as potential threats and risks;

— identify the threats that are most critical to the socio-economic situation in the country;

— assess the capabilities and availability of resources for countering threats;

— determine the necessary forces and means, including weaponry and military equipment, required to achieve the necessary capabilities;

— identify the need for additional resource sources to ensure protection of CI functionality.

After that, conduct analysis and modeling (on computers in the SC) of your scenario for countering threats. As a result of modeling, we will determine:

— causes and sources of security risks;

— probability of occurrence of relevant incidents for identified security risks based on obtained quantitative, qualitative or combined indicators;

— determination of importance (ranking) of security risks based on their indicators;

— comparison of security risks with measures taken to manage them;

— associated security risks;

— measures to prevent the occurrence of security risks;

— the most effective measures to counter such risks;

— measures to minimize possible consequences.

Additionally, different operational scenarios in the SC may depend on whether or not AI is utilized during modeling. AI is increasingly being employed to address unstructured problems in the modern world.

To better understand how a modern SM system should function, let's examine some key issues and management aspects related to protecting the sustainable operation of CI in the power sector.

The author has chosen the power sector as an example to demonstrate the necessity of implementing an SM system using a SC network to ensure the stable functioning of CI. This is because electricity is a fundamental element of both economic activity and life support systems, not only in developed countries but also in our own state.

Thus, we will explore the practical application of SM capabilities for enhancing the protection of CI stability in the power sector.

Ukrainian government and the General Staff of the Armed Forces of Ukraine have made decisions to protect energy infrastructure facilities from Russian missile strikes, drones, and cyberattacks [12]. Energy facilities have been provided with three levels of protection against Russian attacks, including engineering fortifications. Concrete structures are being built around key CIFs managed by Ukrenergo.

When discussing power sector protection, it is essential to address not only what to protect against but also what exactly needs protection. In this case, both physical infrastructure and electricity supply functionality must be safeguarded. The objective for facilities is to minimize vulnerabilities to direct strikes, while the goal for the energy function is to ensure rapid recovery, including resilience against cyber threats.

Ukraine's Unified Energy System (UES) consists of:

— approximately 135 substations with voltage levels ranging from 220 kV to 750 kV;

— nearly 2,000 substations in distribution networks (35–150 kV);

— around 1 million kilometers of power transmission lines.

Since power sector is a fundamental industry, modern information technologies are essential for managing power infrastructure facilities. These technologies must be capable of collecting, transmitting, processing, and displaying critical technological data in real time. This enables personnel to analyze the information and make informed management decisions.

As the frequency and intensity of attacks on the energy sector keep growing, both physical security measures and cybersecurity strategies must be improved and implemented. SM capabilities will facilitate the development of action plans designed to mitigate and neutralize disruptions to critical energy functions.

The relevance of scientifically justifying modern state policy in the field of energy sector protection during the war in Ukraine is determined by several factors:

First, the consequences of missile strikes, accidents, disasters, and other emergencies are becoming increasingly large-scale and dangerous for both the population and the stable functioning of the economy and essential services. Powerful enemy airstrikes that destroy energy sector facilities, along with cyberattacks that compromise the reliability of information and control systems, have led to loss of energy sector resilience. This indicates a certain insufficiency in the Air Defense Forces' capabilities to protect electricity infrastructure as well as cybersecurity measures.

Second, the difficult financial and economic situation caused by the war significantly limits the state's and individual enterprises' ability to build effective physical security systems. To ensure the rational use of available resources, it is necessary to improve the management system. The crisis phenomena that Ukrainian society has faced during military aggression are unprecedented in the modern world. This has demonstrated the importance of a coordinated state policy in the field of infrastructure protection, including electricity infrastructure, and the need for fundamental reforms in this sector.

Third, issues related to administrative functions, organizational structure, operational principles, and development directions of the electricity sector protection system

across the entire national territory still require further clarification of the state's role within this system.

Ensuring the stable operation of the UES requires real-time responses to changes. However, in its operational conditions, there are time constraints on data processing and command transmission, which limit the application of certain critical decisions, including those related to cybersecurity in energy sector information and communication systems.

Unfortunately, threats to the information security of energy sector facilities remain significant (Fig. 5).

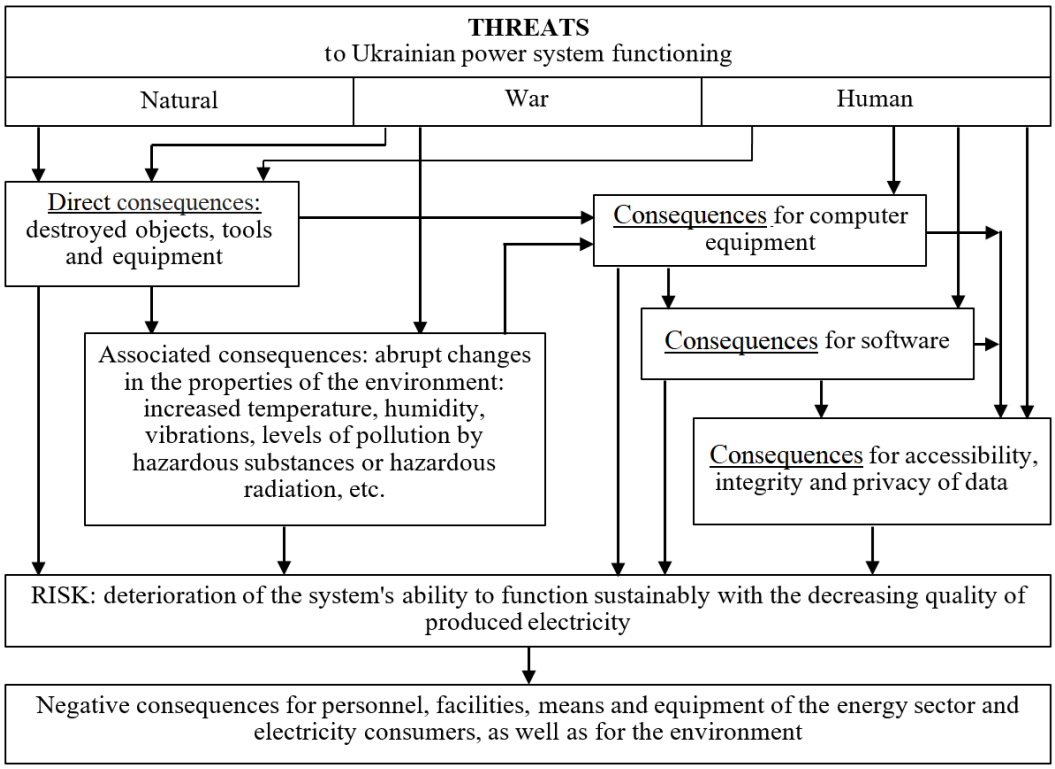

Fig. 5. A model of the impact of threats on the capabilities of the Ukrainian power system

Currently, the requirements for protecting information assets in information management systems of the energy sector are determined by various asset owners.

There are risks of cascading effects in the UES due to the interconnectivity of electrical networks. As a result, local failures in control systems can trigger power outages or degrade electricity quality at a single UES facility. This, in turn, may cause disruptions in electricity supply across multiple regions and even at the national level.

Existing cybersecurity approaches in energy infrastructure facilities still do not fully meet the requirements for securing critical technological information, which is legally defined for protection. Key issues include:

— mismatch between the level of electronic communication infrastructure development and modern security requirements;

— insufficient development of organizational and technical infrastructure for ensuring cybersecurity and cyber defense of critical information infrastructure and electronic information resources;

— ineffective response to military and terrorist cyber threats (Fig. 6), which may lead to significant disruptions in the management of the energy system;

— insufficient organizational and technical infrastructure for cybersecurity and cyber defense, which further weakens protection against potential threats.

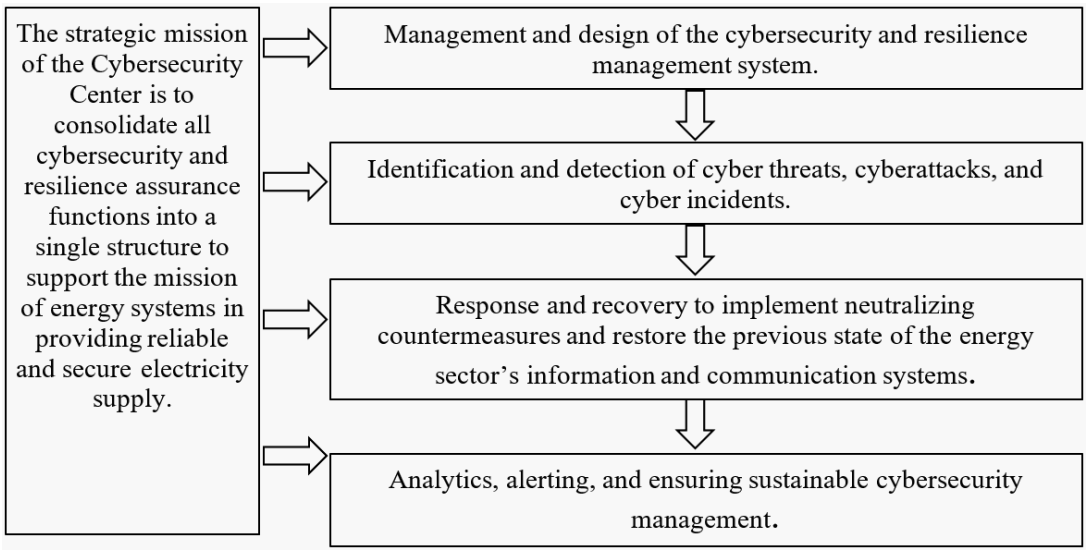

Fig. 6. Tasks and functions of cybersecurity in the electric power industry

The main task of cybersecurity is the consolidation of all cybersecurity functions [13].

A modern management system in the energy sector requires the implementation of cutting-edge SM technologies that incorporate the latest scientific advancements, specifically:

— introduction of a strategic management system, including scenario-based market modeling;

— implementation of resource management principles in energy sector governance;

— personnel training to operate under new functional models and modern scientific-technical support;

— enhancement of the public-private partnership system, among other initiatives [13].

Based on the above, we see a clear necessity for the integration of modern information technologies, including computers, AI capabilities, and other automation tools — ranging from individual automated workstations to the creation of computerized situational centers (CSCs) at energy facilities, which would then be connected into a unified network.

Within these CSCs, it is essential to develop scenario-based approaches for leveraging advanced SM technologies. This includes creating databases, expert systems, and knowledge bases, as well as integrating AI agents into decision-making processes.

To achieve this, all energy sector management facilities, regardless of ownership type (depending on the facility's importance and significance), and relevant state au-

thorities must implement automation tools in the form of CSCs to support decision-making processes.

In future, these CSCs should be integrated into a unified SM network for Ukraine's UES. This would enable rapid access to objective information regarding the current situation, as well as availability of critical energy infrastructure equipment, its production, delivery, and deployment capabilities, both domestically and among allied nations supporting Ukraine.

Conclusions

It is necessary to proactively develop scenarios of potential threats, risks, and preventive measures for protection against aerial strikes, sabotage attacks, etc. Highly professional courses of action are also required to overcome the consequences of potential losses resulting from the destruction of CIFs and the disruption of their functions.

SCs, as modern and future information technologies, represent an opportunity for the development of the management system within the executive authorities of Ukraine through the implementation of situational management that incorporates AI capabilities, including the use of AI agents.

The development and use of scenarios and the implementation of AI agents will become one of the main directions of development of decision support systems. To improve the use of AI capabilities, it is necessary to create appropriate knowledge bases. The integration of the AI agent function call based on a large language model (LLM) will transform it from a passive responder into an active solver to the problem of protecting the CIF.

To protect the state's CI, it is necessary to create a unified network of SCs of central executive authorities, CIFs, and specialized analytical centers that provide the possibility of collegial modeling and decision-making.

It would be advisable, for the purpose of coordinating organizational and information-analytical actions to protect the sustainable functioning of the state's CI and ensure the livelihood of society, to establish a national crisis management center within the Cabinet of Ministers of Ukraine.

It is necessary to implement modern innovative methods and forms of management for the sustainable operation of the electric power industry. It is appropriate to improve the system for managing the protection and security of the electric power sector and its resilience at the national (statewide) level, as well as at the sectoral (departmental), local, and facility levels.

The author of the article is fully aware that only certain aspects of the discussed problem could be presented in a single publication. Much remains to be clarified and supplemented in the future.

1. On Critical Infrastructure: Law of Ukraine dated November 16, 2021 No. 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

2. Morozov A.O., Yashchenko V.A. Situational Centers. Information Technologies of the Future. Kyiv: SP «Intertehnodruk», 2008. 332 p.

3. On the Improvement of the Network of Situational Centers and the Digital Transformation of the National Security and Defense Sphere: Decree of the President of Ukraine dated June 18, 2021 No. 260/2021. URL: https://www.president.gov.ua/documents/2602021-39225

4. Resolution of the Cabinet of Ministers of Ukraine dated July 11, 2023 No. 705 «Situation center network issues». URL: https://zakon.rada.gov.ua/laws/show/705-2023-%D0%BF

5. Morozov A.O., Kuzmenko G.Ye., Lytvynov V.A. Situational Centers: Theory and Practice. Kyiv: SP «Intertehnodruk», 2009. 346 pp.

6. Serrano Luis. Grokking Machine Learning. Simon and Schuster, 2021. 350 p.

7. Pykalo O. Ukraina rozrobyt vlasnu velyku movnu model ShI do kintsia 2025 roku – Fedorov. *Forbes Ukraine*. 2025. URL: https://forbes.ua/news/ukraina-rozrobit-ukrainomovnu-llm-model-do-kintsya-2025-roku-fedorov-31032025-28433

8. Mytnyk M. Chinese developers have released a new artificial intelligence, Manus. *Ukrainian technology portal iTechua*. 2025. URL: https://itechua.com/news/278491.

9. Davydova O. Scenario modeling — the optimal approach to planning. *Hlobalni ta natsionalni problemy ekonomiky.* MNU im. V.O. Sukhomlynskoho. 2014. No 2. P. 493–498. URL: http://global-national.in.ua/vipusk-1-2014/141.pdf

10. Klebanova T.S., Gurjanova L.S., Trunova T. N., Smirnova A.Ju. Scenario modeling in regional development management. *Business Inform*. 2012. No. 10. P. 60–65.

11. Lande D.V., Boichenko A.V. Organization of Analytical Activity Based on the Scenario Approach. *Data Rec., Storage & Processing.* 2015. Vol. 17, No. 1. P. 68–76. https://doi.org/10.35681/1560-9189.2015.17.1.100308

12. The Ukrainian Government and the General Staff of the Armed Forces of Ukraine. On November 20, 2023, they adopted a decision on the protection of energy infrastructure facilities. URL: https://rubryka.com/2023/11/21/v-ukrayini-energoob-yekty-otrymaly-try-rivni-zahystu-u-chomu-rishennya/

13. Hulak Ye.G. Models and Methods for Ensuring the Guarantee Capability and Cybersecurity of Information and Communication Systems in the Energy Sector: Dissertation for the Degree of Doctor of Philosophy: 05.13.21. Kyiv, 2024. 190 p.

Received 23.03.2025