Information & Security: An International Journal

Sukhodolia, vol.40: 2, 2018, 107-119 https://doi.org/10.11610/isij.4008

IMPLEMENTATION OF THE CONCEPT OF CRITICAL INFRASTRUCTURE PROTECTION IN UKRAINE: ACHIEVEMENTS AND CHALLENGES

Oleksandr SUKHODOLIA

Abstract: Enhancing critical infrastructure protection and resilience has become a national security policy priority in many countries. World best practices demonstrate the need to build a system of critical infrastructure protection capable to prevent, mitigate and respond to all types of threats (i.e. natural, man-made, criminal and terrorist threats) and their possible combinations. The establishment of such a system requires legislative definition of its fundamental principles of operation, application of common approaches to the management of critical infrastructure security at all levels, clear identification of the principles of interaction and cooperation among state authorities, private business, society and the public. Despite the progress achieved by Ukraine in implementing the new approach, there is still a lot of work ahead to build the effective state system of critical infrastructure protection. For Ukraine, the successful implementation of the system will mean the transition to a new level of state management in this field based on modern approaches to security risks management, optimal use of available resources, and timely response to security and safety incidents and crises in resolving national security and defense issues.

Keywords: critical infrastructure protection, resilience, crisis management

Introduction

Ukraine has well-developed state system of physical protection of separated objects of critical infrastructure (hereinafter – CI). The most effective system was established within nuclear energy sector Ukraine, which is in full compliance with international standards on protection of nuclear facilities. Following up international support and internal 'historical' legacy of physical protection Ukraine managed to develop a reliable system for physical protection of nuclear facilities and materials that gave an additional push to efforts of developing a new system of critical infrastructure protection (hereinafter – CIP) in Ukraine. However, the system of physical protection of other sectors of CIP, namely important industrial objects and transport infrastructure was developed for the model of centralized governance and for peacetime. The political and economic reforms in Ukraine (privatization of industry, decentralization of

decision making), the emergence of new actors and the threats to CI (hybrid threats) have stimulated the changes in this field.

The starting point for the development of a new governmental policy on critical infrastructure protection became a development of the Green Paper (hereinafter – GP) on CIP.[1] The final version of the GP was presented by the National Institute for Strategic Studies of Ukraine (hereinafter – NISS) in October 2015 and reflected understanding of the importance of CI stable functionality for national security.[2]

The Concept of a CIP system

The GP shapes a CIP system with focus on shifting government and public attention from 'reactive' policy dealing with crisis consequences to crisis' prevention and contingency planning, strengthening coordination of different actors involved and establishing effective public-private partnership relations in the field.

Shortly, eight important points are fixed by GP:

1. Introducing term "critical infrastructure" into the legislation, namely "*Critical infrastructure of Ukraine shall mean and include systems and resources, whether physical or virtual, that support functions and services whose disruption will cause most severe negative effects for the activity of the society, socioeconomic development of the country and national security.*"[2, 7] Currently, the absence of the term leads to confusion in the list of CI assets to be protected what creates difficulties in the effective coordination of efforts between different ministries and agencies.

2. Defining the purpose of a CIP system, namely to ensure a stable functioning of infrastructure and by this to guarantee supply of goods and services vital to the population, society, business and government.

3. Shifting the emphasis from the currently dominating dimension of physical protection of systems and facilities to enhancing the resilience of CI. Under critical infrastructure resilience GP understand "*capability of reliably operating in the normal mode, adapt to continuously changing environment, withstand and quickly recover from accidents and technical failures, malicious acts, natural calamities and hazardous natural phenomena.*"[2, 7]

4. Specifying the categories of threats according to the "all hazard approach" (natural disasters, emergencies and technical failures, malicious activities) focusing on elements of CI that could be targeted (physical elements, management and communication systems, personnel).

5. Fixing trilateral goal of a state CIP system, namely to ensure: a) smooth functioning of CI (reliability); b) ability to resist against the threats (resistibility); c) ability to

recover operations in case of interruption within a certain time period (resilience). All these aspects should be reflected in contingency planning of CI operators as well.

6. Suggesting criteria to assign certain facilities and systems to list of CI.

7. Requiring predefinition of some CIP elements:

- operational regimes of CI (procedures) and modes of control of a CIP system (both at a state and CI operator levels);
- related organizational, institutional, economic and law regimes of CI facilities functioning in accordance with levels of threats.

8. Suggesting design of institutional and organizational structure and responsibilities of the involved parties.

It was proposed to establish four operational modes of CI functioning and CIP system's regimes:

- "Green" – early warning (threat anticipation and prevention) – normal mode of CI functioning; normal legal and economic regimes. A CIP system works on anticipation and prevention of threats, and utilizes early warning tools;
- "Yellow" – alert (threat determent and CI protection) – normal mode of CI functioning; normal legal and economic regimes. In case of threat identification, a CIP system switches to early warning regime of CI functioning. A CIP system works for protection of selected facilities within designed object protection system (internal resources), checks on preparedness of external resources in order to prevent threat realization;
- "Orange" – threat suppression and CI disruption mitigation – special mode of CI functioning, some restrictions in legal and economy regimes (similar regimes on power market have been introduced in Ukraine few times in the period 2014–2017). A CIP system works for suppression of threats and mitigation of negative impact on CI functioning. A CIP system utilizes needed external forces and resources to eliminate threats and negative consequences;
- "Blue" – threat response and recovery of the CI functioning – special mode of CI functioning; serious restrictions in legal and economy regimes. A CIP system works for recovering the ability of CI to perform their functions for society and state;
- "Red" – threat response – special mode of CI functioning; serious restrictions in legal and economy regimes; state could take full control over the regime of CI functioning. A CIP system utilizes all available forces and resources within special period (war, emergency) of governance (legal framework).

In order to determine the level of requirements for protection of CI, distribution of powers and responsibilities among all involved stakeholders it was proposed to assign objects of infrastructure to categories, as follows:

- Category I: the objects critically important for the state and having national importance, multiple and complex ties with other infrastructure objects. These objects are to be put on the list of the CI objects for protection and resource allocation (including state resources) in accordance with legally determined requirements;
- Category II: the objects critically important at the regional level. Their destruction and damage will lead to the crisis situations at regional level. These objects have to be protected in a framework of private-public partnership according to the legally determined requirements;
- Category III: important infrastructure objects. These objects have to be protected in a framework of private-public partnership;
- Category IV: necessary infrastructure objects. It is the responsibility of operators to assure a stable functioning of objects.

Explanation of proposed approach for a CIP system design, together with comparison of responsibility of available in Ukraine systems is given on Fig. 1.

The Challenges of Introducing the CIP System

The planned pace of GP development and practical implementation of its provisions were accelerated due to "hybrid war" against Ukraine. The "Green Paper" project, starting as scientific research activity, was transformed into practical task to launch a new security policy of Ukraine.[3] In addition, new tools of warfare stipulated the need to reassess the paradigm of CIP, shifting attention from "protection" to "resilience" of CI. As well, it was emphasized that the buildup of the national CIP system needs to aim at enhancing the resilience of the infrastructure against hazards of any kind.

This situation brought challenges of available capacity and the acceptance of the initiative. Any change in existing systems, setting new set of tasks and goals is very challenging for every country, but for Ukraine in times of war it became extremely difficult. There was the need to create a "critical mass" of support for the new concept in government agencies and ministries, as well as capability of staff to accomplish the set tasks in a limited timeframe, emergency, lack of resources and knowledge in the field.

Another challenge was the need to specify the role/place of the CIP concept within the national security domain as well as the tasks and duties of all involved actors.

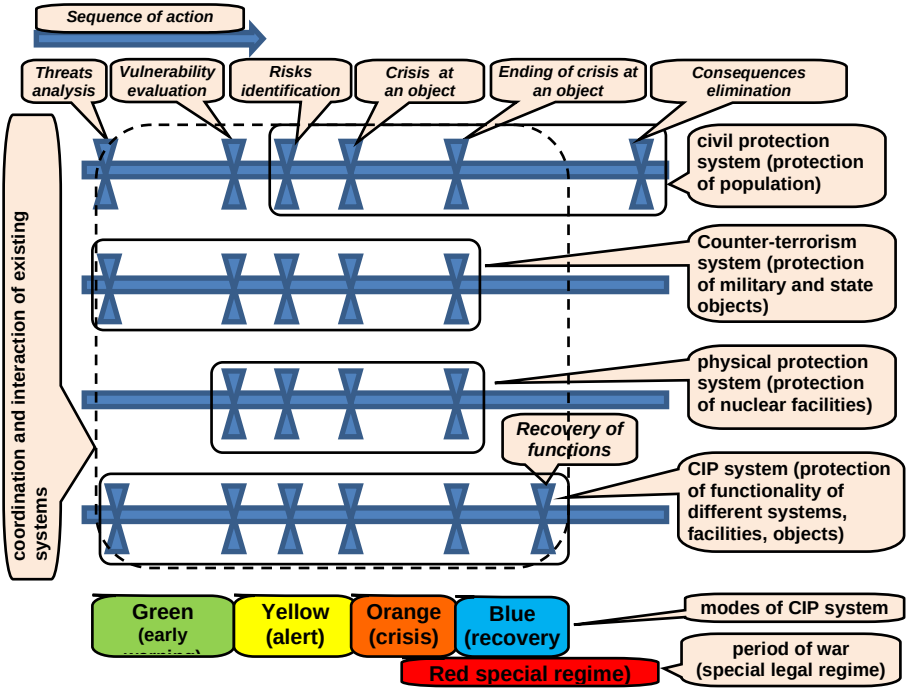

Figure 1: Critical Infrastructure Protection: involved stakeholders' responsibility.

The existing state systems which covered some areas of CIP demonstrated some resistance to rapid change. Therefore, it is so important to combine efforts of the most relevant systems that have been established in Ukraine earlier:

- The Unified State System for Civil Protection;
- The State Physical Protection System;
- The Unified State System for Prevention of, Responding to and Suppressing Terrorist Acts and Mitigating their Consequences;
- the National Cyber Security System, which is under creation in pursuance of the recently adopted Cyber Security Strategy of Ukraine (approved by Decree of the President of Ukraine no. 96/2016 of 15 March 2016), the objectives of which are tightly connected with the CIP.

Currently, it is hardly possible for Ukraine to fully reshape the existing institutional structure of the agencies involved in CIP. Therefore, the GP proposes to differentiate events related to CI malfunctioning according to main duties of the existed systems. That could create possibility of combining efforts of different systems by developing procedures of interaction and coordination.

One of the priority tasks of CIP system development in a near future is to clarify the procedures of interagency coordination, interaction and exchange information taking into account existence of competition for "influence" in the current structure of governmental bodies. So, "unintended events" like technical errors, accidents, natural disaster, etc. could be managed with the help of existing civil protection system while "targeted (malicious) actions" require the development of "prediction" and use of tools to respond to terrorist threats by the relevant counter-terrorism system.

From the formal point of view, the adoption of such approach partially solves the problem of coordination in the field of CIP, especially in the cases of emergency. However, it is impossible to establish a comprehensive CIP system totally based on existing systems, like the existing systems of civil protection or counter-terrorism. There have to be an entity that would develop and operate procedures of interagency interaction and exchange information on CIP.

The NISS analysis indicated that the best organizational approach consists of establishment of national center for crisis management and critical infrastructure protection which has to be tasked with informational, analytical and methodological support of a CIP system and combining efforts of the existed system through national and sectorial situational centers as part of the national network of distributed situational centers (crisis centers within different systems). The added value of a CIP system is to present institutional basis for "preventive and contingency planning" to secure CI stable functionality and resilience.

The urgency of the issue and the awareness of problems with the CIP system support the achievement of general understanding of the need for further actions in this field. CIP became one of the priorities of newly adopted National Security Strategy of Ukraine, which introduced priorities of further activity in this regard. In fact, at present there is consensus on the need to implement contingency planning and the risk management concept into Ukraine's legislation and practice of governance with the aim to prevent interruption of CI functioning.

Further, other legislative acts of strategic importance were adopted, tasking various government agencies and ministries on CIP.

First of all, there is the decision of the National Security and Defense Council of Ukraine of 29 December 2016 "On improvement of measures to ensure the protection of critical infrastructure objects," approved by Presidential Decree no. 8/2017.[4]

By this decision the Government of Ukraine is tasked to ensure comprehensive improvement of the legal basis for critical infrastructure protection and to establish a state administrative system for its security. The Cabinet of Ministers of Ukraine was tasked:

1) within two months to draft, with the participation of the National Institute for Strategic Studies, and approve the concept of establishing the state critical infrastructure system and a roadmap for its implementation;

2) within two months after approval of the concept of establishing the state critical infrastructure system with the participation of the Security Service of Ukraine, the Foreign Intelligence Service of Ukraine and the National Bank of Ukraine to draft the Law of Ukraine "On Critical Infrastructure and Its Protection" with the aim to legislatively resolve all issues regarding establishing the state critical infrastructure protection system.

The draft of "The Concept of Building a State Critical Infrastructure Protection System in Ukraine" was developed by the NISS and delivered to the Government of Ukraine in March of 2017. The unofficial translation of the Concept is available in the book "Developing the Critical Infrastructure Protection System in Ukraine" (D.Bobro, S. Kondratov, V.Horbulin. O.Sukhodolia, 2017, 56–68).[5]

The Concept was approved by Resolution of the Cabinet of Ministers of Ukraine on December 6, 2017.[6] This resolution not only fixed the conceptual approach to establishing of the state system as proposed by NISS, but also opened the way for development of the respective draft law.

In the summer of 2017, the Ministry of Economic Development and Trade of Ukraine established inter-ministerial working groups to prepare needed draft of legal acts required by the National Security and Defense Council decision. After approving the Concept, this group focused on the development of the draft of Law of Ukraine "On Critical Infrastructure and Its Protection."

The Cabinet of Ministers of Ukraine and the Ministry of Internal Affairs adopted legal acts clarifying the role of the National Police and the National Guard in providing protection to some CI objects, while the Ukrainian parliament adopted the Law of Ukraine "On Basic Principles of Providing Cyber Security of Ukraine." Other ministries mentioned in GP as responsible for sectors of CI started paying attention to their area of responsibility as well.

In order to develop the methodology for designating infrastructure objects to critical energy infrastructure and to prepare recommendations on procedures of such objects passportization and categorization the interagency working group was also established under the Ministry of Energy and Coal Industry. As well, the Ministry works on establishing an Energy Crisis Center that has to provide information exchange between all involved agencies responsible for stable and resilient functioning of the energy sector of Ukraine.

Separately, the Security Service of Ukraine took an active role in the implementation of the CIP concept. In accordance with priorities of reform of Security and Defense Sector of Ukraine, the Security Service of Ukraine was tasked to provide threat identification, intelligence informational exchange and coordination of efforts of government agencies on some aspects of CIP.

Other important decision of the National Security and Defense Council that incorporated the new approach to CIP were adopted, namely: Concept of Further Development of the Security and Defense Sector of Ukraine; Cyber Security Strategy of Ukraine; Measures to neutralize energy security threats and to strengthen critical infrastructure protection.

This success encountered another challenge to the process of CIP implementation, specifically overcoming habitual routine and traditional procedures from government bodies as well as operators of CI, namely:

- changing the habitual practice of involved actors;
- developing new tools and their application under time and resource constraints;
- getting new knowledge and skills;
- ensuring mutually supporting actions of all involved actors (state, public, industry).

NISS, in order to find a way to resolve this problem, launched a set of raising awareness, education and training events.

Support for the Process of CIP Conceptualization

The process of CIP Concept implementation received assistance to facilitate the identification of the elements needed to make easier the move ahead.

1. Involve experts from the private sector and state agencies in designing a CIP system. It helps to shape right ideas of the GP as well as create support in order to facilitate the "transfer" of new concepts into the activity of public entities. At the same time, it helps clarify provisions and escape legal traps and create common understanding of future cooperation between institutions.

2. Use existing institutions. The institutional structure which exists today, for example civil protection or counter-terror system could be used for implementation of a new CIP concept. However, the focus of the activity should be tuned. Countering malicious acts, like acts of sabotage, could be resolved by means of the counter-terror system. However, CIP should cover also other types of targeted actions that include political decisions of other states too (like a decision of Russia to halt energy supply

to Ukraine). Ensuring continuity of functioning of the infrastructure is not protection of habitual conditions of citizens' life what supposed to remain the domain of civil protection service.

3. Engage existing tools. Some threats to the stable functioning of CI could be generated by malicious actions, but the big part of threat is generated by technical errors, accidents, natural disaster, etc. In general, a CIP system should be capable to propose two-level set of measures, namely measures aimed at reducing threats and resolving crises. The goal of the CIP system is to minimize the risks of interrupting the operation of CI through building tools of protection (with priority on reliability and resistibility), as well as to prepare options for quick restoration of CI functionality (priority on resilience).

4. Demonstrate the added value of a CIP system. The growing threats from malicious actions against CI require a proactive policy. A CIP system will assess the risks to continuity of infrastructure functioning through cooperation of government as well as operators of CEI through establishing close private-public partnership decreasing state expenditures. That target requires the establishment of "preventive action planning" giving special attention not only to build physical protection at all stages of the life cycle of CI (design, location, construction, installation, commissioning, operation and liquidation of consequences) but also to develop interconnectivity of CI, availability of needed reserves, involvement of private sector resources.

5. Utilize best practice. International experience and support are very important, especially for countries that are limited in time and resources to develop a CIP system on its own. It is important not only to build on "best practices" in methodology or legislation but also through direct involvement of experts in development pieces of legislation. For example, concerning the energy sector of Ukraine in 2015, the elements of "contingency planning" were developed by team of experts from USA, Canada and EU countries and implemented into the draft "Plan for functioning of Energy Sector of Ukraine in the winter period of 2015/2016" and "Plan for achieving energy sustainability of Ukraine."

Other relevant examples of international cooperation within the CIP concept development includes:

- development of conceptual policy papers on CI and development of framework legislation. The GP on CIP has been created by the NISS of Ukraine with the active support of experts from NATO countries;
- education of staff of ministries and agencies involved in CIP system functioning. The NATO Professional Development Program has vastly contributed and supported the NISS in organizing series of seminars on CIP from 2013 till 2015;

- training the staff of ministries and agencies. So, the NISS and the NATO Energy Security Centre of Excellence organized a table-top exercise on Critical Energy Infrastructure Protection, held in Ukraine in October 2017.

Further Development of the CIP System

Taking into account the diverse and complicated character of the objectives to be accomplished within the framework of the CIP Concept implementation, it is reasonable to examine the process on different stages that could be implemented upon previous progress and availability of resources.

At this point Ukraine would use the experience of other countries, especially from Eastern and Central Europe, which few years earlier have been executing the same task. In this context it would be very useful to utilize the advice of experts from NATO countries that were delivered to Ukraine while supporting development of the "Green Paper." The experience of eastern neighbors of Ukraine displays the need for:

- gradual inclusion of new components into the CIP system; proportionality of resource allocation on base of risk analysis; development of reliable instruments of cooperation between all stakeholders (public private partnership); providing information security protection (Ratchev, 2015);[7]
- legal basis for imposing obligations on CI operators regarding the protection of listed CI objects. Operators should be obliged to prepare critical infrastructure protection plans. Such plans should have full description of protection in six areas: Physical, Technical, Personnel, IT, Legal, Recovery (Brzozowski, 2015); [8]
- distribution of responsibilities of operators, local and national authorities within the CIP system; proportionality in designing protection measures, in order to ensure the best results with the least investment of scarce resources; aiming protection measures at strengthening resilience (Mureșan and Georgescu, 2015);[9]
- reliable system of cooperation and coordination of involved stakeholders, securing flows of information and knowledge; continuous learning (Tagarev, 2015).[10]

These recommendations were implemented in the three-stage process of developing Ukrainian CIP capabilities. The short-term objectives of further development of the CIP system in Ukraine include development and approval of the basic legislative and relevant regulations, which will create the foundations for state CI system functioning, including a competent authority determined by the law to coordinate activities aiming at CIP. Among mid-term objectives are the measures to establish organizational and legal as well as functional and structural foundations for the state CIP sys-

tem functioning. The Long-term objectives prescribe completion of institutional and legal structure of the CIP system and creation of tools of efficient operation maintenance of the system.

Among the priorities in development of the legislative and regulatory basis for a state CIP system are [5]:

- appointment of an authority responsible for shaping and implementation of State's policy in the field of CIP under peaceful conditions and in a special period of time, as well as authority to bear responsibility for administrative, technical and scientific support of a national center for crisis management and critical infrastructure protection;
- development and approval of the list of CI sectors and charging specific agencies with responsibility for their protection;
- development, approval and introduction of the list and categories of CI objects;
- development, approval and introduction of the methodology for designating infrastructure objects as CI, procedures of their passportization and categorization;
- ensuring unified methodological foundations for relevant activities carried out by all parties involved in operation of the state CIP system;
- development of regulations on technical requirements for critical infrastructure operation as well as their stable functioning in different modes;
- establishment of public-private partnership to improve security and resilience of national CI that provides for clear legislative regulations on responsibilities and duties distribution among authorities and owners (operators) of the CI objects;
- creation of an efficient system designed for gathering information on risks and threats against CI, its analysis and processing;
- establishment of a national training and re-training system for CIP.

Conclusion

Despite the tangible results achieved in CIP Concept implementation, there is still a lot of work ahead to build the effective state system of critical infrastructure protection in Ukraine. The future efforts have to focus on establishing a framework of robust interaction, the adequate levels of cooperation and interaction among all involved stakeholders, well-developed and sustainable public-private partnership, adequate training and education capabilities and involvement in international cooperation in this field.

The major expected result from CIP Concept can provide a due level of CIP in Ukraine against all types of threats as well as efficient response to security incidents, mitigation of consequences and quick recovery of CIP objects operation relying. Success in building the state CIP system will mean transition to a new level of state management in this field based on modern approaches to security risks management, the optimum use of available resources, flexibility and timely responding to security and safety incidents and crisis due and, in particular, active support from society, local communities, media and NGOs involved in resolving national security and defense issues.

References

1 Sergiy Kondratov, "Introducing Critical Infrastructure Protection Concept in Ukraine: Lessons to Learn," in *Zelena knyha z pytan zakhystu krytychoy infrastructuru,* ed. D. Biriukov, S. Kondratov, O. Sukhodolia (Kyiv: NISS, 2015), 57-65.

2 Dmytro Biriukov, Sergiy Kondratov, Oleh Nasvit, and Oleksandr Sukhodolia, *The Green Paper on Critical Infrastructure Protection: Analytical Report* (Kyiv: NISS, 2015), http://en.niss.gov.ua/content/articles/files/Green-Paper-engl-4bd7c.pdf, accessed June 15, 2018.

3 Oleksandr Sukhodolia, "Protection of Critical Infrastructure in Hybrid Warfare: Problems and Priorities of State Policy of Ukraine," *Strategic Priorities* 3 (2016): 62-76. (in Ukrainian)

4 "On Improvement of the Measures to Ensure Protection of Critical Infrastructure Objects," Decree of President of Ukraine № 8/2017, 2017, http://zakon3.rada.gov.ua/laws/show/8/2017, accessed June 15, 2018. (in Ukrainian)

5 Dmytro Bobro, Sergiy Kondratov, Volodymyr Horbulin, and Oleksandr Sukhodolia, eds. *Developing the Critical Infrastructure Protection System in Ukraine* (Kyiv: NISS, 2017), 184, http://en.niss.gov.ua/content/articles/files/Green-Paper-engl-4bd7c.pdf, accessed June 15, 2018.

6 "The Concept of Building a State Critical Infrastructure Protection System in Ukraine," Resolution of the Cabinet Ministers of Ukraine №1009-p, 2017, http://zakon2.rada.gov.ua/laws/show/1009-2017-%D1%80, accessed February 2, 2018. (in Ukrainian)

7 Valeri Ratchev, "On the European Experience in Critical Infrastructure Protection," in *Zelena knyha z pytan zakhystu krytychoy infrastructuru*," ed. D. Biriukov, S. Kondratov, O. Sukhodolia (Kyiv: NISS, 2015), 155-156. (in Ukrainian)

8 Krzysztof Brzozowski, "On the Experience of Poland in the Development of Critical Infrastructure Protection System," in *Zelena knyha z pytan zakhystu krytychoy infrastructuru*, ed. D. Biriukov, S. Kondratov, O. Sukhodolia (Kyiv: NISS, 2015), 156-158. (in Ukrainian)

[9] Liviu Mureşan and Alexandru Georgescu, "Critical Infrastructure Protection – Romanian Contributions and Experiences," in *Zelena knyha z pytan zakhystu kritychoy infrastructuru*, ed. D. Biriukov, S. Kondratov, O. Sukhodolia (Kyiv: NISS, 2015), 93-106. (in Ukrainian)

[10] Todor Tagarev, "Critical Infrastructure Protection: The Challenges of Establishing Interagency Cooperation," in *Zelena knyha z pytan zakhystu kritychoy infrastructuru*, ed. D. Biriukov, S. Kondratov, O. Sukhodolia (Kyiv: NISS, 2015), 158-161. (in Ukrainian)

About the Author

Oleksandr Sukhodolia graduated the National Technical University of Ukraine "Kyiv Polytechnic Institute" (NTUU "KPI") in 1994, Department of Electrical Power Engineering and Automatics. Oleksandr received a Ph.D degree in Electrical Engineering in 1999 from NTUU "KPI" and D.Sc degree in Public Administration in 2007 from the National Academy of Public Administration. He has extensive experience in public service and higher education. He served as a Head of Department and Deputy Head of the State Committee of Ukraine on Energy Conservation (1998-2003), Deputy Head of Energy Security Department at a Secretariat of the National Security and Defense Council of Ukraine (2007-20011). In 2001-2013 he was teaching Energy Efficiency and Energy Policy at the Energy Saving and Energy Management Institute of Ukraine (NTUU "KPI") and, in 2012-2016, the Energy Security at the National Academy of Public Administration. From 2012 Oleksandr Sukhodolia works at the National Institute for Strategic Studies (Ukraine) at the position of the Head of Energy Security and Technogenic Safety Department. In last few years his research interests focused on the energy security and critical energy infrastructure protection. He has published widely on energy efficiency, energy and national security, critical infrastructure protection. He authored the book *Energy efficiency in the context of national security: research methodology and implementation mechanisms* (2006) and co-authored the "*Green Paper on Critical Infrastructure Protection in Ukraine*" (2015) and the monograph "*World Hybrid War: Ukrainian Front*" (2017), and "*Developing the critical infrastructure protection system in Ukraine*" (2017).