Rafał Wróbel - Zuzanna Derenda

THE CONCEPT OF CRITICAL INFRASTRUCTURE PROTECTION IN POLAND FOR YEARS 2015-2017

Abstract

Introduction: This article deals with the concept of the critical infrastructure protection in Poland, showing the period 2015-2017. This includes a National Program on the Protection of Critical Infrastructures, and the article also introduces other legal solutions that have a direct impact on critical infrastructure. Methods: The paper contributed to the detailed study and analysis of Polish literature and various laws. Result: As a result of the paper it can be the shown the responsibility and the tasks of the critical infrastructure coordinators, as well as the methods for improving the protection of the infrastructures and their legislative background.

Keywords: National Critical Infrastructure Protection Program, critical infrastructure, concept of protection, update, departments of government, the vision of Council of Ministers.

A KRITIKUS INFRASTRUKTÚRA VÉDELEM AKTUÁLIS HELYZETE LENGYELORSZÁGBAN

Absztrakt

Bevezetés: A cikk Lengyelország kritikus infrastruktúra védelmének koncepciójával foglalkozik 2015-2017 közötti időszakot bemutatva. Ennek része egy Nemzeti Program a Létfontosságú Infrastruktúrák Védelméről. Emellett a cikk bemutat más jogi megoldásokat is, amelyek közvetlen hatással vannak a kritikus infrastruktúra. Módszertan: A cikk elkészítéséhez nagymértékben hozzájárult a lengyel szakirodalom és különböző jogszabályok részletes tanulmányozása és elemzése. Eredmény: A cikk eredményeként megfogalmazható a

létfontosságú rendszerelemek koordinátorainak felelőssége és feladatai, valamint az infrastruktúrák védelmének javítását szolgáló módszerek és azok jogszabályi háttere.

Kulcsszavak: Nemzeti Kritikus Infrastruktúra Védelmi Program, kritikus infrastruktúra, védelmi koncepció, kormányzati osztályok, Lengyelország

1. INTRODUCTION

Contemporary concept of critical infrastructure protection in Poland is based on the assumption that this is implemented within a crisis management system. Detailed tasks related to the protection of critical infrastructure are defined in the Act of 26 April 2007 on Crisis Management. [1] The abovementioned legal act, referred to as the mother-in-law in the area of crisis management, defines that the vision of the Council of Ministers for Critical Infrastructure Protection (CIP) in Poland is defined by the National Critical Infrastructure Protection Program (NCIPP). This program is prepared by the Director of the Governmental Center for Security (GCS Director) in cooperation with the ministers and heads of the central offices responsible for critical infrastructure systems (CI systems) and with national security ministers. The version of the program, prepared in 2011, is fully categorized, so the first widely available version was released in 2013. The National Critical Infrastructure Protection Program for 2013-2015, in November 2015, according to the two-year planning period, has been updated. Its current version concerns the presentation of priorities, objectives, requirements and standards for 2015-2017. At the same time, November 2015 seems to be crucial for the concept of critical infrastructure protection for other reasons. The swearing of the new created government and the implementation of the act of 17 November 2015 on the amendment of the act on the Departments of Government Administration and some other acts introduces changes in the responsibility of selected ministers responsible for critical infrastructure systems. [2] The presentation of changes contained in the National Critical Infrastructure Protection Program, as well as the identification of key changes resulting from the amendment of the Act on the Departments of Government Administration, are objects of interest to particular sections of the discussion.

2. LEGAL BASIS FOR CRITICAL INFRASTURCTURE PROTECTION

The issue of critical infrastructure and its protection has been reflected in the provisions of the Act of 26 April 2007. [3] It defines basic definitions for critical infrastructure protection, the purpose of creating the National Critical Infrastructure Protection Program, the principles for designating national and European critical infrastructure as well as critical infrastructure protection tasks. These tasks include:

- collection and processing information on critical infrastructure threats,
- development and implementation procedures in the event of critical infrastructure threats,
- restoring critical infrastructure,
- cooperation between public administration and owners and owners of spontaneous and dependent facilities, installations or facilities of critical infrastructure for its protection. [4]

In addition to the elements mentioned above, the act also clarifies the obligations of critical infrastructure operators to protect their infrastructure by preparing and implementing critical infrastructure protection plans and maintaining their own backup systems that ensure the security and maintenance of the infrastructure until it is fully restored. At the same time, in implementing the requirements of the Council of Europe Directive, [5] the act obliged these critical infrastructure operators to designate a person responsible for maintaining contacts with the relevant Critical Infrastructure Protection Authority.

Responsibilities for Critical Infrastructure Operations are also defined in relation to the Director of the Governmental Center for Security and Ministers responsible for Critical Infrastructure Systems and relevant for national security issues.

The abovementioned law provides delegations with detailed solutions on how to fulfill obligations and cooperation in the area of the National Critical Infrastructure Protection Program by public administrations and national security services with critical infrastructure operators,[6] as well as how to create, update and structure the critical infrastructure protection plans developed by operators of the same, the conditions and procedures for recognizing the fulfillment of the obligation to have a plan that meets the requirements of the critical infrastructure protection plan. [7]

Apart from the listed critical infrastructure elements, the crisis management act, defining the structure of crisis management plans at national, provincial, district and municipality level, indicates that they contain: [8]

- hazards characteristic and risk assessment, including critical infrastructure,
- procedures for the implementation of crisis management tasks, including those related to the protection of critical infrastructure,
- a list of critical infrastructure located in the voivodship, county, municipality for which a crisis management plan is being prepared,
- priorities of the protection and recovery of critical infrastructure.

In addition to the crisis management act and the regulations issued on its basis of 30 April 2010, the following directives on the protection of critical infrastructure include:

- Act of 18 March 2010 on special powers of the Minister responsible for State Treasury and their execution in certain capital companies or groups operating in the sectors of electricity, crude oil and liquid fuels, [9]
- Regulation of the Prime Minister of 14 July 2010 on the plenipotentiary for protection of critical infrastructure, [10]
- Regulation of the Council of Ministers of 3 December 2015 on the Government Plenipotentiary for Strategic Energy Infrastructure.

The first of these legal acts is the legal type of security operation in the energy supply system, energy resources and fuels. The implementing regulation of the discussed law specifies the detailed procedure for appointing and dismissing a representative for critical infrastructure protection. On the other hand, the regulation on the Government Plenipotentiary for Strategic Energy Infrastructure is a new solution, which deals with the proxy exercising certain powers of the State Treasury in relation to the electricity system operator and the gas transmission system operator.

Presented legal solutions should be complemented by legislation that uses a direct reference to critical infrastructure, [12] as well as formal and legal industry solutions that apply to objects, equipment, installations and services considered critical infrastructure. The scope of topic discussed in the title of the article, however, allows us to leave the discussion on industry solutions in particular critical infrastructure systems as separate material.

3. THE VISION OF THE COUNCIL OF MINISTERS IN TERMS OF ENSURING SAFETY OF THE CRITICAL INFRASTRUCTURE

The concept of the Council of Ministers concerning the safe operation of critical infrastructure has been presented in subsequent versions of the National Critical Infrastructure Protection Program. [13] The document defines the scope, objectives, priorities, program rules, addressees, as well as the principles of critical infrastructure identification, the responsibilities of individual program participants, critical infrastructure protection measures, and the transnational dimension. It consists of several parts, including the main part and attachments. The characteristics of the part of the National Critical Infrastructure Protection Program issued in 2013 and its updated version of 2015 are presented in Table 1.

Table 1. Characteristics of the part of the National Critical Infrastructure Protection Program
Source: own elaboration based on [14] and [15].

Document	NCIPP 2013	NCIPP 2015
Main document	National Critical Infrastructure Protection Program - main document (for years 2013-2015)	National Critical Infrastructure Protection Program - main document (for years 2015-2017)
Annex 1	National Critical Infrastructure Protection Program. Annex 1 - Characteristics of critical infrastructure systems	National Critical Infrastructure Protection Program. Annex 1 - Standards for the Safe Operation of Critical Infrastructure - Good Practices and Recommendations
Annex 2	National Critical Infrastructure Protection Program. Annex 2 - Standards for the Safe Operation of Critical Infrastructure - Good Practices and Recommendations	National Critical Infrastructure Protection Program. Annex 2 - Criteria to distinguish installations and services included in critical infrastructure systems [16]
Annex 3	National Critical Infrastructure Protection Program. Annex 3 - Criteria to distinguish installations and services included in critical infrastructure systems [4]	Not applicable

In principle, NCIPP is to create conditions for improving the safety of critical infrastructure in Poland, in particular:

- prevention of disruption to critical infrastructure,
- preparation for situations that may adversely affect critical infrastructure,
- reaction in the event of a critical infrastructure failure (destruction or disruption);
- restoration of critical infrastructure. [1]

Priorities of the program are actions to deepen public-private partnerships between program participants [17], identification of dependencies as well as the assessment of the risk of disruption of the system by critical infrastructure operators in cooperation with the authorities identifying hazards at various levels of public administration in the field and special services, including primarily with the Head of the Internal Security Agency.

Among the many principles of the program, the three most important are three, relating to: co-responsibility, cooperation and trust. [18] [19] [20] Updated in 2015, NCIPP lists the recipients of the program, in particular the government administration, represented by the ministers responsible for critical infrastructure and voivodships, as well as critical infrastructure operators. The list of potentially interested program participants is complemented by other business entities and organizations, the academic community and the public. A list of critical infrastructure facilities based on accepted system criteria and cross-criteria is prepared by the Director of the Governmental Center for Security. The criteria in question are also subject to updating, which is one of the reasons for the changing number of elements in each critical infrastructure system. The number of critical infrastructure elements in 2012-2015, broken down into systems, is presented in Table 2. [21]

Table 2: Number of critical infrastructure elements in 2012-2015 by system. Source: own elaboration based on [22], [23] and [25].

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**Sum**
2012	186	230	60	58	1	5	2	73	20	47	0	682
2013	188	225	56	84	1	69	3	64	20	47	3	760
2014	188	162	54	85	1	67	3	63	20	44	2	689
2015	191	162	53	85	1	67	3	63	20	28	2	675

The majority of facilities, devices, installations and services included in the critical infrastructure over the years have been identified in the energy supply system, energy resources and fuels, and the least in the food supply system. The latter, in addition to the rescue system, are systems where the number of critical infrastructure elements has not changed over the years 2012-2015. In addition to assigning a specific number of critical infrastructure components to each system, there is yet another criterion for CI labeling. Its location determines the division of critical infrastructure elements into voivodships. A sample register, based on the above mentioned criterion, covering the years 2013-2014, is presented in Table 3.

Table 3: Number of critical infrastructure elements in 2013-2014, broken down by voivodship. Source: own elaboration based on [25].

	Lower Silesian	**Kuyavian-Pomeranian**	**Lublin**	**Lubusz**	**Lodzkie**	**Lesser Poland**	**Masovian**	**Opole**	**Subcarpathian**	**Podlachian**	**Pomeranian**	**Silesian**	**Swietokrzyskie**	**Warmian-Masurian**	**Greater Poland**	**West Pomeranian**	**Together**
2013	50	33	31	12	28	40	242	14	36	18	46	76	17	15	59	40	757
2014	45	31	28	11	24	38	221	14	34	17	41	68	15	16	47	36	686

The discussion of critical infrastructure would be incomplete without information that the number of critical infrastructure components in the systems / voivodships can vary for various reasons, among which the most important ones should be considered:

- recalling the CI operators from the decision to recognize (or not) an element that they administer as a critical infrastructure,
- updating the identification criteria,
- legal changes (e.g. related to the change of the minister managing a given department of government administration, within which CI elements were identified).

The National Critical Infrastructure Protection Program defines ministers directing government departments responsible for critical infrastructure systems. Due to the scope of

their initiatives, they have been called coordinators or co-coordinators of CI systems. Ministers responsible for critical infrastructure systems are indicated in Table 4.

Table 4: Ministers responsible for critical infrastructure systems according to the National Critical Infrastructure Protection Program. Source: own elaboration based on NCIPP [25].

Critical infrastructure systems	**Minister responsible for the critical infrastructure system**
Energy, energy raw materials and fuels supply system	Minister of Energy
Communication system	Minister of Digital Affairs Minister of Infrastructure and
ICT networks system	Minister of Digital Affairs
Financial system	Minister of Finance
Food supply system	Minister of Agriculture and Rural Development
Water supply system	Minister of the Environment
Health protection system	Minister of Health
Transport system	Minister of Infrastructure and Construction Minister of Maritime Economy and Inland Sailing
Rescue system	Minister of the Interior and Administration
System ensuring the continuity of the public administration	Minister of Digital Affairs
System of production, stockpiling, storage and use of chemical and radioactive substances, including pipelines of hazardous substances	Minister of the Environment

Critical infrastructure operators include owners and owners of spontaneous or dependent facilities, installations, facilities and critical infrastructure services. They can manage more than one critical infrastructure. To illustrate the differentiation of ownership relationships on

the example of years 2013-2014, Table 5 shows the number of critical infrastructure operators in their respective systems.

Table 5**:** Number of critical infrastructure operators in each system in 2013-2014. Source: own elaboration based on [25].

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**Sum**
2013	27	31	5	7	1	38	3	9	19	26	3	169
2014	28	27	6	7	1	37	3	8	19	24	2	162

The tables 2 and 5 show that in systems with a large CI number, the greatest variability in ownership occurs in the rescue system (20 CI components, 19 CI operators). For comparison, in 2014, one operator was on average:

- within the system ensuring continuity of the public administration – 2 (about 1,8) CI elements (44 CI elements, 24 CI operators);
- within the water supply system – 2 (about 1,8) CI elements (67 CI elements, 37 CI operators);
- within the communication system – 6 CI elements (162 CI elements, 27 CI operators);
- within the energy, energy raw materials and fuels supply system – almost 7 (about 6,7) CI elements (188 CI elements, 28 CI operators);
- within the transport system – 8 (about 7,9) CI elements (63 CI elements, 8 CI operators);
- within the ICT network system – 9 CI elements (54 CI elements, 6 CI operators);
- within the financial system – 12 (about 12,1) CI elements (85 CI elements, 7 CI operators);

The activities of the ministers in charge of CI systems – coordinators / co-coordinators of CI systems were divided into several groups i.e. initiation, implementation, support, consultation and promotion.

Among the initiating actions are those related to:

- initiation and running the legislative process of legislation aimed at improving the functioning of the CI security system within a coordinated system,
- initiation and maintenance of contacts with CI operators,
- implementation of modern critical infrastructure protection techniques,
- stimulation of the participants in the program,
- preparation of strategies to encourage the private sector to participate in the program.

Executive actions come down to:

- assessment of the risk of CI disruption as a result of dysfunction,
- regular analyzes and assessments of the effectiveness of critical infrastructure protection in a CI system,
- organization and operation of the CI forum at the system level,
- participation in the CI protection mechanism,
- organization within the framework of the CI training system for critical infrastructure protection for local governments and the private sector,
- implementation of the continuity managemant system of the public administration
- ensuring that critical infrastructure protection tasks are taken into account in subordinate or subordinate bodies,
- co-ordinate with other coordinators to identify interdependencies between CI,
- providing assistance to GCS in the area of CI identification and implementation and updating of NCIPP,

- co-operate with the authorities overseeing the CI component, if this is not directly within the competence of the minister in question.

In addition to stimulating and executive work, ministers responsible for critical infrastructure systems support other critical infrastructure stakeholders. It takes the form:

- supporting the GCS in building a critical infrastructure protection system,
- support in the organization of exercises at the level of the system to assess the performance of CI protection,
- support activities aimed at recreating CI.

At the same time, CI coordinators agree on critical infrastructure protection plans, advise and provide substantive assistance, as well as assistance in finding experts for CI operators and take action to promote them. The latter concern the promotion at CI level of educational programs on CI protection and awareness raising activities in the area of CI protection. The tasks of the other participants in the program are defined as the subject of separate considerations. One of the pillars of the built-in critical infrastructure protection system is the cooperation of parties interested in achieving a common goal. It is implemented by exchanging all information that may have an impact on achieving the intended purpose, as well as maintaining regular contacts between stakeholders involved in the process of critical infrastructure protection. It is assumed that the model of cooperation in the protection of critical infrastructure contributes to:

- strategic level,
- operational level,
- management level.

The effectiveness of cooperation determines its occurrence at all levels of the critical infrastructure protection system, so the exchange of information constituting the core of the defined cooperation is realized in the following forms:

- critical infrastructure protection forum,
- ongoing information exchange,
- organization of training, conferences, exercises and counseling.

Exchange of information within the forum takes place through the use of national, system and regional forums. The latter is inter-systematic and meets at least three times a year, or more often if needed. The work started during the forum is continued after the meeting.

Current exchange of information takes place within the Critical Infrastructure Protection Mechanism, which relies on the exchange of threat information, increased demand for services or products, and on the Internet platform. Changes made in the organization of trainings, conferences and exercises covered the abolition of duties of the organizer of the exercises (preparation of exercises plans and their reconciliation, determination of purpose and effect of exercises, proper conditions for carrying out exercises, preparation of exercises documentation, providing funds, providing the approved exercise report to GCS Director) and objectives including, among others, objectives and effects, scope of exercise, form / type / range, place of performance, schedule, deadline, scope of documentation.

The updated program also presents an action plan for 2015-2017 of organizational, legal, technical, educational and training nature. The program also makes minor adjustments to the scope of critical infrastructure protection activities under the European Critical Infrastructure Protection Program. The directive on the identification and designation of European Critical Infrastructure and the need for better protection of the protection of the critical infrastructure remains the key element, instruments that fund critical infrastructure protection activities and the concept of cooperation with third countries. [28] CI tasks, with cooperation with other countries and international organizations, include the Government Security Center, the Ministry of Foreign Affairs, the CI system coordinators and the local administration bodies. The GCS Director is responsible for coordinating the program implementation, which annually reports to the Council of Ministers on the effectiveness of the program, taking into account the information received from the ministers in charge of CI and voivodes. An over-estimation of the effectiveness of the program includes measures such as:

- approved CI protection plans,
- CI status protection audits,
- structural and budgetary changes,
- exercises involving emergency and protective services.

Discussion on the scope of changes in the National Critical Infrastructure Protection Program would not be complete without comment on the annexes to the main document. It is clear from the analysis of the contents of Table 1 that existing Annex 1 - Critical Infrastructure

Systems Overview has been withdrawn, replacing the updated version of the existing Annex 2 - Standards for the Safe Operation of Critical Infrastructure - Good Practices and Recommendations. The changes introduced have broadened the scope of practices and recommendations for:

- the most important safety recommendations for all types,
- elements of the business continuity management system in the section on business continuity and recovery plans,
- risk assessment.

Special importance in terms of providing critical infrastructure security are continuity plans consist of crisis management plans, and resources after a disaster, and plans / procedures to recover lost resources. The recovery plans of the latter, taking into account the various causes of resource destruction, should also take into account the different variants of their housing, whether it concerns people, location, technology, information or supply chains. The risk assessment serves to define the IC protection standards and to prioritize actions so it should be done carefully. The critical approach to critical infrastructure protection requires a business case analysis (BIA analysis) in the first place. Its implementation contributes to the estimation of risk in a reliable manner, which may include elements of the methodology presented in ISO 31000 standard. Performing BIA analysis and risk assessment should be done in the following steps: [29]

- identification of processes taking place in the organization,
- identification of critical processes,
- identification of resources,
- identification of threats and vulnerabilities,
- risk analysis,
- risk evaluation.

The presented approach in the preparation of activities favors undisturbed implementation of critical processes of the organization.

4. SUMMARY

The vision of the Council of Ministers in the field of protection of facilities, equipment, installations and services recognized as critical infrastructure is presented in the National Critical Infrastructure Protection Program. Its first wide audience available 2013 edition assumed that the intended goal of the program should be achieved over a 6-year period, with care being taken to update the solution at least every two years. The updated document should take into account changes in the environment as well as security considerations. The NCIPP update, made in 2015, with the 2015-2017 program, extends the scope of the tasks assigned to ministers responsible for critical infrastructure systems, which are no longer referred to as previous hosts / co-hosts and coordinators/co-ordinators. At the same time, changes are perceived in the risk assessment, closely aligned with the continuity system. The current types of critical infrastructure protection have been replaced by security measures. The critical infrastructure protection collaboration model has been reorganized from two to three levels, introducing an additional communication scheme within the CI Protection Mechanism, and making cosmetic corrections to the existing schema. The program removed the responsibilities of the organizers of critical infrastructure protection exercises and their assumptions. The action plan has been redefined two years after the approval of the NCIPP update by the Council of Ministers, scope of activities under the European Critical Infrastructure Protection Program and measures of program effectiveness. The most important changes in the existing program annexes should be the resignation from the annex on the characteristics of critical infrastructure systems, and the extension of the section on good practices and recommendations, especially on ICT security measures, business continuity and recovery plans and risk assessment. Changing the concept of administration allocation to government departments in November 2015 directly affects and supervises certain critical infrastructure systems. Thus, the catalog of ministers responsible for critical infrastructure systems presented in NCIPP 2015 was reviewed in the first half of 2016. The amendment to the act on changings to the act on government departments and some other acts simultaneously creates a delegation to appoint a Government Plenipotentiary for Strategic Energy Infrastructure.

5. REFERENCES

[1] Act of 26 April 2007 *on crisis management* (Journal of Laws of 2007, No. 89, item 590; of 2013, item 1166, of 2015, item 1485).

[2] The Act of 19 November 2015 *on amending the act on the Departments of Government Administration and certain other acts* (Journal of Laws of 2015, item 1960).

[3] Law of 26 April 2007 *on management*..., op. cit.

[4] National Critical Infrastructure Protection Program; Ibidem, art. 6.

[5] Council of Europe Directive 2008/114 / EC of 8 December 2008 on the identification and designation of European Critical Infrastructure and the assessment of the need to improve its protection (OJ L 345, 23/12/2008 P. 0075 -0082).

[6] Ordinance of the Council of Ministers of 30 April 2010 *on the National Critical Infrastructure Protection Program* (Journal of Laws of 2010 No. 83, item 541).

[7] Ordinance of the Council of Ministers of 30 April 2010 *on critical infrastructure protection plans* (Journal of Laws of 2010 No. 83 item 542).

[8] R. Wróbel, M. Mytkowska, *Critical Infrastructure Protection and the obligation to develop plans and programs under the crisis management act*, "AON Doctoral Lectures 2012, No. 2.

[9] Act of 18 March 2010 *on the specific powers of the Minister responsible for State Treasury and their execution in certain capital companies or capital groups operating in the electricity, oil and liquid fuels sectors* (Journal of Laws of 2010 No. 65, item 404).

[10] Regulation of the Prime Minister of 14 July 2010 *on the plenipotentiary for critical infrastructure protection* (Journal of Laws of 2010, No. 135, item 906).

[11] Regulation of the Council of Ministers of 3 December 2015 *on the Government Plenipotentiary for Strategic Energy Infrastructure* (Journal of Laws of 2015, item 2116).

[12] Examples of this includes the Announcement of the Marshal of the Sejm of the Republic of Poland of 28 July 2015 *on the publication of the uniform text of the Strategic Reserve Act* (Journal of Laws of 2015, item 1229), art. 3, 4, 8 (pt. 9), 18.

[13] GCS, National Infrastructure Protection Program 2013 and National Program for Critical Infrastructure Protection for 2015.

[14] National Critical Infrastructure Protection Program - Main Document, the Governmental Center for Security, Warsaw 2013.

[15] National Critical Infrastructure Protection Program - Main Document, the Governmental Center for Security, Warsaw 2015.

[16] Document protected under the provisions of the Act of 5 August 2010 *on the protection of classified information* (Journal of Laws of 2010, No. 182, item 1228).

[17] R. Wróbel, *Critical Infrastructure and its common character [in:] Safety Research Paradigms. Crisis management in theory and practice*, Pub. Higher School of Security, Poznań 2013, p. 686-697.

[18] The division of responsibility resulting from the function fulfilled by the critical infrastructure - on the one hand the menial nature of the administration and, on the other, the commercial activity of the private sector.

[19] Coherent, reciprocal, coordinated action to achieve a specific goal, avoiding duplication of effort.

[20] The conviction that the reason for doing so is the pursuit of a shared mission, defined by public administrations and infrastructure operators, to address the critical need to improve the security of critical infrastructure.

[21] Critical infrastructure elements within the meaning of the article mean facilities, equipment, installations and services considered critical infrastructure based on accepted CI identification criteria.

[22] Kulik I., Security of European Critical Infrastructure Facilities in maritime areas [in:] Kustra W. (ed.), Armed Forces Cooperation with Public Administration in maritime areas, Pub. SRWO, Warsaw 2012.

[23] Skomra W., Materials from the speech on "Cooperation between the administration and the private sector in the area of business continuity", 1st National Congress of Business Continuity Management, Jachranka (26-27 March 2015).

[25] Szewczyk T., Materials from the speech on "National Critical Infrastructure Protection Program - past experience", Conference "Ensuring continuity of functioning of state organs in the face of present threats", Szczytno (23-24 September 2014).

[26] R. Wróbel, I. Kulik, *Decision Making in the Preparation of Critical Infrastructure Protection Institutions* [in:] Piątek Z., Truchan J. (Ed.), *Technologies in Critical Infrastructure Protection - External State of the European Union*, Pub. Association of Defense Movements, Szczytno 2013, p. 199-210.

[27] National Critical Infrastructure Protection Program - Main Document, the Governmental Center for Security, Warsaw 2015.

[28] Program "Prevention, Preparedness and Consequence Management of Terrorism and Other Security Risk" - CIPS in the years 2007-2013 and the "Internal Security Fund" - ISF in 2014-2020

[29] The PN-ISO 31000:2012 standard developed by the Technical Committee No. 6 on Management Systems and approved by the President of Polish Committee for Standardization on 27 February 2012 is a literal translation of the International Standard 31000:2009. The PN-ISO 31000: 2012 standard is dedicated to risk-taking organizations that are forced to manage it.

Sr. Cpl. PhD Eng. Rafał Wróbel

The Main School of Fire Service, Unit of Analysis Civil Safety, Faculty of Civil Safety Engineering, Varsó, Lengyelország

E-mail: rafalwrobel.sgsp@gmail.com

Orcid: 0000-0002-2338-0267

Zuzanna Derenda

The Main School of Fire Service, Faculty of Civil Safety Engineering, Varsó, Lengyelország

E-mail: zuzanna.derenda@gmail.com

Orcid: 0000-0002-5482-3964

A kézirat benyújtása: 2017. 03.12.

A kézirat elfogadása: 2017.07.10.