THE IMPACT OF RELIABILITY AND CONTINUITY OF OPERATIONS ON CRISIS MANAGEMENT INFORMATION SYSTEMS

Faustyna KLOCEK
Michał KORZENIEWSKI

Wojskowa Akademia Techniczna[1*]

Abstract. In today's world, the IT systems have a huge influence on the functioning of public administration. IT systems become indispensable when managing processes and providing public services. There are very exposed to cyber attacks from other countries. It is said that there may be about 1000 attacks around the world every hour. This make difficult or impossible to work that systems, which ensure efficient functioning of the state. Crisis management system is particularly important for our security. That system allow to prevent threats and mitigating the consequences of disasters. Its integral part is reliable IT systems that are part of critical infrastructure. Therefore, we strive to ensure the continuity of the system, because only with the continuity of operations we are able to successfully and effectively operate in a crisis situation. An element of efficient public administration is reliable IT systems for crisis management. After a crisis situation, a huge amount of information is stored and processed. To facilitate the management of information, are created new tools that would be support decision making. One of them is Integrated Management Information Systems, thanks to which it is possible to prevent crises on a national scale. They work with virtual network technologies with the support of artificial intelligence.
Keywords: new technologies, IT security systems, crisis management, cyberspace.

Nowadays, in an urbanised, automated, computerised world there are more and more threats that affect the functioning of entire societies, institutions or individuals. Often we do not realize how much our everyday life depends on the efficient operations of energy, banking or IT systems and how closely they are related. Ensuring the continuity of operations of these systems requires effort on the part of enterprises, as well as public administration. Continuity of operations means the ability to continue action in any one the following situations: natural disasters, unfortunate accidents, terrorist attacks or grave failure.

Public administration also creates a system, which in case of danger, ensures the continuity on the functioning of the state – this is known as crisis management system. Each year, the dependence of all branches of the economy on all types of information systems increases. These systems are becoming more and more complicated and maintaining their continuity of operations is increasingly necessary for the efficient functioning of a state.

---

[1] Studenci Studiów Bezpieczeństwa Narodowego, IOiZ WCY, WAT w Warszawie.

In accordance with the Act of Crisis Management of 26 April 2007 critical infrastructure is defined as "systems and their functionally, interconnected objects including construction objects, devices, installations, important services for the security of the state and its citizens, and to ensure the efficient functioning of public administration bodies, as well as institutions and entrepreneurs"[2]. Critical infrastructure includes for example IT network system. It is also worth noting that critical infrastructure is highly exposed to various types of threats, which are either the result of forces of nature or the negative and harmful actions of people. If the infrastructure element is disrupted, it will have negative implications for citizens and the country itself. Therefore, the duty of public administration is reliability in the protection of this infrastructure and take all reasonable steps to mitigate the effects of damages and easily remove them if necessary[3].

What does the term "system' mean? It is widely used in many different aspects of science and practice. It may refer to objects, phenomena and processes occurring in nature or created by people. The concept of the system is of particular importance in the theories of cybernetic systems. The system may also be a set of methods of operation and performance of complex activities, for example a deductme system[4], as well as a set of various organisational rules, accepted norms and/or rules in force in the area of a given subject matter (for example a tax system, moral system)[5].

Why is it so important to ensure the continuity of the system? Only with the continuity of operations we are able to successfully and effectively operate in a crisis situation. Polish law emphasises the importance of this systemic feature, to guarantee the continuity of operations in public administration[6]. This is describe in the Act of Crisis Management of 26 April 2007. Protection of critical infrastructure requires operational continuity there of in order to prevent the occurrence of negative effects[7].

Business Continuity Management (BCM) prescribes a series of actions, behaviors and decision-making processes which take place within an organisation of the system in a situation of crisis[8]. These are interrelated actions and common dependencies that cannot allow the interruption of the continuity of operations operation. This process is realised not only in the event of a catastrophe, but also preventing phenomena

2 *Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r.*, Dz.U. 2007 nr 89, poz. 590.

3 T. Kaczmarek, G. Ćwiek, *Ryzyko kryzysu a ciągłość działania*, wyd. Difin, Warszawa 2009, s. 20.

4 Deductme system is a set of statements composed of axioms (sentences accepted without proof). In the theory of deductme systems examine the consistency pf absoluteness and deducibility.

5 https://encyklopedia.pwn.pl/haslo/;398219.

6 Ustawa z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 nr 89, poz. 590).

7 *Ocena ryzyka na potrzeby zarządzania kryzysowego. Raport o zagrożeniach bezpieczeństwa narodowego*, RCB, Warszawa 2013.

8 J. Zawiła-Niedźwiecki, *Dobre praktyki czy teoria zapewniania ciągłości działania*, Politechniki Warszawska, Instytut Organizacji Systemów Produkcyjnych 2012.

threatening the system, preparing to take control and contain the phenomenon and removal consequences of its occurrence[9].

The continuity of operations management contains problem operational risk triad, which consists of: resource security, operational risk management and operation continuity. These issues are interconnected because the identification, analysis and assessment of risks as well as risks are conducted in order to set guidelines to adequately protect against negative effects and preventive action in case of crisis situations. The main goal is also to ensure business continuity[10].

Currently, business continuity management is a challenge in every branch, including security. In this sector, ensuring business continuity should be of special importance due to the growing importance of various security areas and emerging new threats. Amongst them are cyberattacks and problems of reliable operation of devices and systems, which are used to transmit information. Extensive experience in the field of computer science both verifies scientific findings and shapes professional practice in the design of devices and systems with the assumed reliability and in the creation of organisational solutions taking into account the expected unreliability of the used devices and information systems.

Reliability of operation continuity means striving for excellent administration work, even if an emergency situation occurs. The operation continuity of administration is achieved by sufficient IT systems, the ability to respond rapidly to disturbances occurring and to protect the most necessary processes and resources essential for the maintenance and renewal of business. Presently the reliability of operation continuity of administration entities is violated by the impact of operational risk factors, namely the threats to which the organisation is susceptible due to imperfect adaptation of internal processes, poor training of employees or incorrect management of resources. In the last few years, the issue of reliability of operation continuity has been connected to the issues of the type of risk that should be identified, estimate of finances and the likelihood of crisis situations. „The ability to govern depends on the continuity of the administration functioning. When the government loses control in a crisis situation, it loses social trust and, consequently, the ability to defend itself"[11]. It is important to maintain basic public services so that citizens feel safe in their country.

We already know that maintaining business continuity is important. The question is how to ensure it? Every state and enterprise creates a plan in the event of a crisis situation that could cause the interruption of the continuity of operation of the systems. The purpose of creating such a plan is its duration. The extent to which a particular

[9] T. Kaczmarek, G. Ćwiek, *Ryzyko kryzysu*…, op. cit., s. 30.

[10] https://www.pbsg.pl/ciaglosc-dzialania, dostęp z dnia: 10.03.2018.

[11] Zastępca sekretarza generalnego NATO Patrick Turner podczas międzynarodowej konferencji zorganizowanej przez Rządowe Centrum Bezpieczeństwa, http://www.samorzad.lex.pl/czytaj/-/artykul/specjalisci-o-ciaglosci-dzialania-administracji-w-sytuacjach-kryzysowych, dostęp z dnia: 6.01.2018.

company or organisation constantly changes to adapt to fluctuating market conditions requires the correction of many of its parameters[12]. An extremely important element of each plan is to describe detailed solutions that must be used as part of a specific strategy. Each detailed plan is a scenario of processes and actions undertaken during a crisis situation. However, even the most detailed plan is not enough to ensure the continuity of the system. The plan should be supplemented with regular trainings and training of employees as well as the implementation of modern IT systems[13]. Implementation of an IT system is a process that must be well planned from the content and cost side. The project, which is accurately and realistically estimated has the best chance of ending successfully and preventing future crisis situations. Machines, electronic systems (including data processing systems, archiving systems, and security systems) and other devices must have regular tests. This allows to detect errors that can then be repaired or removed. Sometimes, after testing, you may find that you need to write a new plan. Not every test must lead to new changes to the plan but such activities should at least provide information on their effectiveness in the event of a crisis[14].

The management of present organizations is closely related to information systems (IS), which have been applied in many areas of their functioning. Such systems are implemented in public administration with a view to improving processes, which in turn will ensure the quality of public services provided. IT systems become indispensable when managing processes and providing public services[15].

The relevant institutions will provide security, when they have a potential to enable processes to be carried out. In crisis management, there are also various processes, but in order to achieve them, we need various components at the entrance, for example staff, capital, infrastructure, information and technology. These components stimulate the set-up of new goals and transformation of existing processes which in turn create a blanket of security corresponding with an original goal. To be able to make an assessment, we need to analyse the criteria we have used. One of them is reliability. This is the ability to use basic functions in the computerised world, full of threats in cyberspace, which are characterised by high dynamics. This means that they must be systematically monitored and analysed. Therefore, the process of risk assessment in ministries, central offices and voivodeships must be carried out in a systematic manner. Preparatory activities will focus on identifying system resources and the possibilities of their use. If we have that reliability in a useful category, public administration activities should be based mainly on prepared, precise plans and laws in order to quickly,

[12] T.T. Kaczmarek, G. Ćwiek, *Ryzyko kryzysu…*, op. cit., s. 48.

[13] Ibidem, s. 60-61.

[14] Ibidem, s. 136-145.

[15] E. Ziemba, I. Obłąk, *Informatyczne wsparcie procesów w administracji publicznej*, [w:] *Technologie informatyczne w administracji publicznej*, Zeszyt 33/2014, red. A. Kobyliński, A. Sobczak, „Roczniki Kolegium Analiz Ekonomicznych SGH", Warszawa, s. 619.

reliably and effectively prevent action, if necessary. Such a plan is the National Crisis Management Plan, which applies if there is no possibility to take effective action through the provincial level (as a result of lack of adequate forces and resources). These are situations in which central level actions are necessary (usually coordinated activities of several ministries and central offices). KPZK includes characteristics of threats and risk assessment of their occurrence, tasks and responsibilities of participants in the form of a safety net, list of forces and measures planned to be used in crisis situations, tasks and emergency response procedures, as well as many other components that form a pattern of action during a threat. The reasons for the business continuity violation refer to the origins of the risk and lead to the conclusion that it is impossible to maintain operations of continuity and that the occurrence of disturbances is natural and unavoidable. The theory of business continuity in crisis management should be aimed at creating emergency, crisis or so-called plans of civil defense. Improvement of solutions through tests, exercises and analysis of incidents is required[16].

The rapid development of teleinformatics created information society with tools such as the Internet, computer networks or dedicated decision support systems (DSS-Decision Support System). It has enabled communication and access to the ability to analyse information on an unprecedented scale. The large amount of data that is analysed during the crisis situation forces you to develop new concepts of using the already stored information as well as to create completely new, intelligent tools that will help you effectively manage your information. Integrated Management Information Systems have been present for at least two decades and constitute the main source of information and support in the decisions being made. Over the years, they have evolved so as to include an increasingly larger area, which allows support on a wider scale and achievement of better results[17].

One of the essential stages in shaping security is the initial stage of diagnosis. The model being built for this purposes will be reduced to the identification and assessment of threats based on the apparatus and system engineering tools. This problem concerns a particular type of threats that generate critical situations and, in the longer term, crisis situations. System security must be considered in the aspects of external threats as well as impacts on the environment and outflow on shaping the security of the society. The most important thing is that the system is safe for itself and the immediate environment and system environment. Because safety is a derivative of threats, every attempt to classify them must refer to the root causes. The basis of the term Integrated Management Information System is the concept of an IT system and it is defined as a time-and-space-separated information

[16] http://rcb.gov.pl/ksiega-dobrych-praktyk-w-zakresie-zarzadzania-ciagloscia-dzialania/, dostęp z dnia: 10.03.2018.

[17] Z. Banaszak, S. Kłos, J. Mleczko, *Zintegrowane systemy zarządzania*, PWE Polskie Wydawnictwo Ekonomiczne, 2016, s. 41.

processing system, which is a collection of intentionally related elements, which are: data sources, methods of their collection and processing, information flow channels, material resources and people carrying out the processing and destination of information. A standard integrated system is a universal software. It contains functions that fit most organisations. For specific requirements, the system can be adapted to individual needs. This is also the case with the title crisis management system due to which it is possible to prevent crisis or, if they occur, to effectively minimise their effects. It would be impossible on the national scale if it were not for highly automated crisis response systems that operate using virtual network technologies with the support of artificial intelligence, information technology or microelectronics. These systems are not limited to automated monitoring based on automatic sensors and sensors that have the function of early warning. Some of them carry out professional preventive and anti-crisis activities, they also make executive decisions[18]. Modern crisis response systems are a guarantee of public, technical or political security. Due to the huge rank and high complexity of the security problems of large systems, their research should be based on scientific theoretical foundations and proven track methods. The random nature of threats and the enormous dynamics of security processes mean that universally recognised scientific methods, such as the theory of stochastic processes, methods of mass service theory and computer simulation methods, are suitable for more effective analysis of these phenomena[19]. Particularly interesting results are achieved by using various types of operational research, specialised network programming or mathematical programming. The main advantage of the graph theory and its tools is the utility in the process of modeling phenomena and dynamic systems. We are talking here about the usefulness of natural and social systems, where strict mathematical methods have proved to be too unreliable. Graph theory is a very practical and effective tool for system modeling. But that theory is also a bit complicated when consider system relations (information or energy).

Each system and its model in the form of a graph contains two basic components: X, a set of highlighted structural and organisational elements, and R – a description of the organisation of this set of elements, showing the type of dependence between elements. A systematic approach requires that such a model has the purpose of the action for which the organizational and functional structure has been established.

Another field of science, the theory of mass service, is based on the theory of stochastic processes. Although the theoretical assumptions of mass service systems

[18] A. Januszewski, *Funkcjonalność informatycznych systemów zarządzania*, t. 1, *Zintegrowane systemy transakcyjne*, t. 2, Warszawa 2017.

[19] P. Zaskórski, K. Szwarc, *Bezpieczeństwo zasobów informacyjnych determinantą informatycznych technologii zarządzania*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki", nr 9, rok 7, 2013, s. 37-52.

are very complicated and require mathematical advancement, their defeat provides us with a device for testing various praxeological systems. First of all, we will treat the crisis response system as a mass service system in which there are one or more service channels that we can visualise as the process of emergence and manifestation of various types of crisis threats in a certain environment. In order to keep systemic assumptions about the homogeneity of the stream of reports, considering the complexity and difficulty of submitting threats to a given classification, it is necessary to limit the scope and category of applications to a minimum. Crisis response systems are service stations for individual notifications and customers that destabilise the existing security situation. Reports like emergency threats, clients at the office can be "served", "directed" to another queue in anticipation of service being controlled to limit the consequences of waiting. They can also "leave" the crisis response system without any control which can result in serious consequences. In practice, this means getting out completely out of control. In rationally serviced crisis response systems, this situation should not take place as it threatens to escalate the threat. The prospective development direction is to improve the functioning and operation of mass systems with the help of scientific methods and research tools. The integration of crisis management systems and mass service systems can be increased by incorporating computer simulation techniques. The most promising is the possibility of contributing to a significant improvement of the functioning of the crisis management system. It is possible through the use of computer simulations which is indispensable in research on large scale and dynamics of activities. The concept of simulation in science means artificial reproduction of symbolic data of the correct object, process or system. Instead of experimenting on a real object which generates costs, and often is simply impossible, we can present the object in the form of a mathematical model and proceed to simulation. In the case of the most effective computer simulation, the model is saved in the form of a programming language and run as a simulation program. When changing the parameters, we can observe and make a detailed analysis in many variants. With a high complexity of calculations, it does not cause major difficulties in identification. Simulation tests are much cheaper, and above all safer and faster than observations. An important parameter of simulation is time, thanks to which it is suitable for testing complex processes and physical or atmospheric phenomena. It consists in reproducing fragments of the examined reality in the order consistent with the passage of time. However, the simulation technique has some drawbacks. Even the most accurate model corresponds to reality only in a certain approximation, which affects the results of the research. However, to summarize the spectrum of advantages, it definitely dominates the difficulties and that is why computer simulation is today the most effective method of scientific research[20].

[20] K. Ficoń, *Inżynieria zarządzania kryzysowego: podejście systemowe*, BEL Studio 2016, s. 16.

The world in which we live constantly forces us to face the threats – natural or technical, which due to the development of civilization often have no impact. At each level of administration, they build security systems that are aimed at reducing the probability of crisis situations. One of the possibilities of lowering the chance of occurrence of a threat is education. On the one hand, education of the society which has an impact on increasing awareness of threats, on the other proper training of emergency services for efficient and proper help in emergency situations and employees of government and self-government administration responsible for coordinating and supporting emergency services in operations. „It is necessary to ensure the continuity of the government and the entire administration in the event of terrorist and hybrid threats, and even during the classic war. Digitization of services is accompanied by threats from cybercriminals, e.g. deliberate destruction of data, their unauthorized downloading, and a break in the operation of systems supporting emergency services and medical services could be extremely severe" [21]. Currently, public administration in Poland is passing through the process of computerization. Reliability and continuity of operations is crucial in managing processes in public administration. The reason is even the fact that management is much more complicated in public administration than in business organisations. Public administration has a strictly determined organisational structure, and decisions are made over a long period of time. In addition, legal considerations make processes less flexible as rigid frameworks for implementing these processes are imposed. Improving IT systems in public administration is therefore much harder. Nevertheless, the importance of taking up processes through IT systems is high, which is why the informatisation of public administration needs to be increased. Additionally, the integration of crisis management information systems will enable the implementation of a project combining Polish administration with other European administrations through the IDA program (Interchange of Data Between Administrations) [22].

When creating an integrated crisis management system attention should be paid to factors that improve the quality of IT systems. To correctly perform this process:

- define the goals, strategies and principles of system security,
- define security requirements and guidelines,
- identify and analyse threats,
- identify and analyse the vulnerability of IT resources,
- identify and analyse the risk,
- specify appropriate safeguards,
- monitor the implementation process and security operations[23].

[21] http://www.gazetaprawna.pl/artykuly/977803,specjalisci-o-ciaglosci-dzialania-administracji-w-sytuacjach-kryzysowych.html, dostęp: 06.01.2018.

[22] E. Ziemba, I. Obłąk, *Informatyczne wsparcie procesów w administracji…*, op. cit., s. 625.

[23] http://www.politechnika.lublin.pl/dydaktyka/pliki/wyk/PSK_IMUZ/PSK_IMUZ_W5_lato2007.pdf, dostęp z dnia 10.03.2018.

The correct implementation of all these activities is essential for effective secrity management. It should be remembered that the IT system will only be correct if security becomes an integral part of it. It is impossible to consider this issue separately as it should be a feature of all processes from the very beginning.

For the IT system to be reliable attention should be paid to its basic features:

- confidentiality – data protection against disclosure of fuzzy stones,
- integrity of protection against unauthorised changes,
- accessibility – access to information, but only for cultivated persons,
- authenticity – verification of the identity and resource resources,
- reliability – a guarantee of expected system behavior and obtained results,
- correctness – a system that meets the tasks and is free of errors,
- reading and project management,
- a real collection of resources,
- interacting with other systems[24].

To create a good IT system you have to start with the appropriate security classification. System security can be divided into physical, technical, personal and organisational aspects. The basic protection should start with proper physical preparation. So what is the security of every computer that is connected to the integrated information system? A computer can be considered safe when we can rely on it and its system software behaves in accordance with the expectations we have defined. We can expect from such device that data initially entered into it will exist in a few weeks and will not be read by unauthorised persons[25]. It is important to define the security policy for the persons using the system as well as the system itself. In addition, an effective security system also plays a significant role in determining security since a computer equipped with the best software and the latest technical equipment remains unusable if it is not adequately protected against adverse physical phenomena. It should be ensured that the rooms are free from hazards such as:

- electrostatic and atmospheric discharges (electrifying liner or dissipation for electric discharge),
- strong electromagnetic fields (created by eg. transformer stations, treatment devices and electricity, etc.),
- fires, floods etc.[26]

Server rooms and computers should be provided with a constant temperature, humidity and other parameters determined by the manufacturers of computer hardware. In addition to the above, these devices should be equipped with replacement

[24] Ibidem.

[25] S. Garfinkel, A. Schwartz, G. Spafford, *Practical Unix & Internet Security*, 3rd Edition, O'Reilly & Associates, Sebastopol 2003, s. 30.

[26] https://www.up.lublin.pl/files/pracownicy/polityka_bezpieczenstwa_teleinformatycznego.pdf, dostęp z dnia 02.03.2018.

devices generating electricity in the event of interruption of energy supply, e.g. power generators, which achieve full efficiency in just several dozen seconds after commissioning. Cabinets in which physical data bases will be stored (i.e. on magnetic carriers) should be adequately protected against external factors that may lead to data damage or loss.

An additional protection against data loss is also duplication of discs and databases. RAID(Redundant Array of Independent Disk) has been created for this particular purpose. It involves the cooperation of two or more hard drives to provide greater capabilities that are unachievable using one disk. These devices are used to increase reliability, efficiency of data transmission and availability of space as a whole. Currently, there are many different types of this device.

RAID 0, or the banding of disks. The device realizes the recording simultaneously on two disks. System performance increases (simultaneous saving of subsequent data blocks). The use of this technology does not increase the level of security because if any disk is damaged we can irretrievably lose the data on it[27].

RAID 1 – mirroring. Each block of data is saved on two different disks. This technique provides a high level of security, but the total disk capacity is 50%[28].

RAID 3 – stripe set with parity, i.e. a strip with a separate disk storing parity bits. This technology ensures efficiency and security increase and allows you to restore data after failure of one of the disks. Any modification of the data requires updating the parity disk's records, which may cause a drop in the system's performance.

RAID 5 – parity bits scattered on all disks. The technology similar to RAID 3 – but it does not cause a drop in performance caused by waiting for writing to the parity disk, it allows an increase in efficiency and ensures data security.

Another solution is backup. Currently, there are three different forms of copy:

- A full copy is based on copying of all files. The disadvantage of this solution is the time-consuming backup time for very fast data recovery.
- An incremental copy consists of copying files that have been modified. It enters a modern game.
- Copy (s) and then up. The disadvantage of this solution is the requirement to restore the last level of the backup and the last differential copy. Such a solution allows for even faster announcement than in a backup[29].

Why is it important to adequately secure the crisis management system by mirroring and backing up data? The system should always have access to all information, especially in the event of a crisis situation, in order to be reliable and have the ability

[27] http://macierze-netapp.pl/technologie/rodzaje-raid.html, dostęp z dnia: 10.03.2018.

[28] https://dyski.cdrinfo.pl/artykuly/raid-konfiguracja-macierzy-dyskowych/strona2.php, dostęp z dnia 10.03.2018.

[29] http://www.komputerswiat.pl/artykuly/redakcyjne/2016/11/wszystko-o-backupie.aspx, dostęp z dnia: 10.03.2018.

to act continuously. It is unacceptable for a situation in which any data will be lost as it can lead to a powerful catastrophe with tragic consequences.

Another problem is adequate physical protection of the IT system against unauthorised persons. All locations of technical devices necessary for the proper operation and functioning of the system should be located in hard to reach spaces, access to which will be difficult for undesirable people. The room should be equipped with alarm systems and devices preventing free movement and making it more difficult to take property. The access to such rooms should be secured by appropriate access control.

We can examine the level of IT system security on the basis of two methods. The first of them is the so-called the security class as part of the standards contained in the Orange Book(developed by the US Department of Defense). This book contains descriptions of criteria from the assignment of analysed systems to security classes and information on how to correctly perform IT security analysis. The second method of assessing the level of security is to perform expert opinions known as risk analysis, which is assessed taking into account the strong probability of occurrence of threats[30].

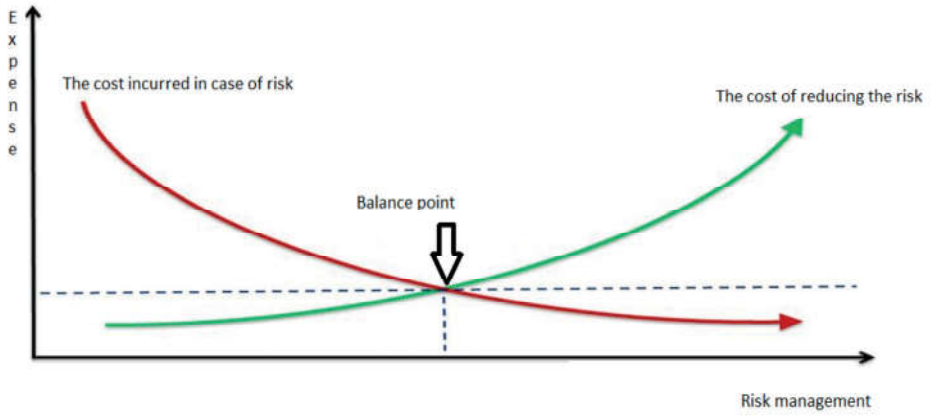
When researching the problems of IT crisis management systems, one must bear in mind that it is practically impossible to achieve total security. This is directly related to the fact that computer systems often remain "open" and attempt to implement them without access to the Internet would lose their sense. On the other hand, the costs of creating absolute security could be so high that it would cost the creation of the system many times, which is why it is so important to correctly estimate the costs and benefits of the crisis management system in order to determine the balance between costs incurred in the event of an incident; the costs of reducing this risk[31].

In order for the IT crisis management system to work properly, all users of this system should be familiar with the requirements necessary to take effective protection of IT resources. Over the last years, the number of incidents related to the functioning of information systems has been constantly growing. The advancing technological development and computerization of further aspects of everyday life entails further threats that have not previously occurred on such a large scale. Potential attackers can be divided into the following categories:

- Hackers, seniors for satisfied and tested their skills,
- Terrorists who through blackmail and theft have the opportunity to achieve goals,
- Spies, who try to steal information and technologies for other countries,
- Vandals who want to demolish and spend for pleasure.

[30] http://www.ae.krakow.pl/~wiluszt/WSEI/SEMINARIA/wsei-2006-trynka-bezpieczenstwo-ro.pdf, dostęp z dnia: 10.03.2018.

[31] http://www.ae.krakow.pl/~wiluszt/WSEI/SEMINARIA/wsei-2006-trynka-bezpieczenstwo-ro.pdf, dostęp z dnia: 10.03.2018.



Source: Own elaboration

The motives of the aggressors are different but they can be categorized as follows:

- financial benefits,
- politics and ideology,
- revenge,
- propaganda,
- vandalism[32].

The National Center for Crisis Management, which also fulfills its functions thanks to the efficiency of IT systems, is the Government Center for Security. The creation of RCB was a significant step in the construction of an effective and comprehensive crisis management system. One of the basic tasks of RCB is to analyse the threats occurring at the moment based on information obtained from all crisis centers and on the basis of data received from international partners. The main role here is played by coordinating the flow of information about threats[33]. To make this possible, the IT system must be reliable. The Government Security Center houses the Faculty of Information Technology and Communications. Their task is to maintain the continuity of functioning and administration of public information and communication systems and the OPAL Classified Internet Service. One of the main undertakings is organisation and supervision over the implementation of tasks designated by the policy of protection of cyberspace in the Republic of Poland. It is also necessary to implement information security management systems[34].

[32] http://www.pszw.edu.pl/images/publikacje/t014_pszw_2008_zajdel_michalcewicz_-_analiza_zabezpieczen_systemow_informatycznych.pdf, dostęp z dnia: 10.03.2018.
[33] http://www.isok.gov.pl/pl/rzadowe-centrum-bezpieczenstwa-rcb, dostęp z dnia 5.03.2018.
[34] https://rcb.gov.pl/wydzial-informatyki-i-lacznosci/, dostęp z dnia: 5.03.2018.

The reliability and continuity of the crisis management information systems will make it possible to provide an effective system for the protection of the country. One of the projects aimed at supporting the protection of society, the economy and the environment against extraordinary threats, as well as supporting decision-making in the event of dangerous events, is the IT System of Country Protection (ISOK). The ISOK System will include, among others, preliminary flood risk assessment, flood hazard maps and flood risk maps. In addition, geospatial data related to meteorological and other hazards will be published in the System. In accordance with the assumptions made in the ISOK system, the Central Node serves all recipients of data and services at all levels of administration in the country[35].

The threat to the operation of information systems is the fact that the number of threats, attacks and computer incidents has increased significantly recently. Almost every day, every organization encounters computer attacks. Many of them are not aware that they are subject to an attack, others only act in the event of an incident, while organisations with a high level of consciousness plan their response to the threat ahead of time while maintaining a constant readiness to actively defend their resources[36]. The application of appropriate practices and mechanisms that minimise data loss and allow for the fastest possible restoration of the service after a failure makes the organisation trustworthy. Continuity plans for IT systems should be developed in the event of a serious incident (hardware failure, software error, loss or destruction of data or other disasters affecting the functioning of the system). Their launch should take place in crisis situations. It is necessary to determine the conditions for launching such a plan and proceeding as a result of a failure or a cyber-attack that would disrupt the reliability of the system[37].

BIBLIOGRAPHY

[1] Banaszak Z., Kłos S., Mleczko J., *Zintegrowane systemy zarządzania*, PWE Polskie Wydawnictwo Ekonomiczne, 2016.

[2] Ficoń K., *Inżynieria zarządzania kryzysowego: podejście systemowe*, BEL Studio 2016.

[3] Garfinkel S., Schwartz A., Spafford G., *Practical Unix & Internet Security 3rd Edition*, O'Reilly & Associates, Sebastopol 2003.

[4] Januszewski A., *Funkcjonalność informatycznych systemów zarządzania*, t. 1, *Zintegrowane systemy transakcyjne*, t. 2, Warszawa 2017.

[5] Kaczmarek T., Ćwiek G., *Ryzyko kryzysu a ciągłość działania*, wyd. Difin, Warszawa 2009.

[35] http://www.isok.gov.pl/pl/szukaj?tag=rcb, dostęp z dnia: 10.03.2018.

[36] https://rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/, dostęp z dnia: 12.03.2018.

[37] https://www.pbsg.pl/ciaglosc-dzialania-systemow-informatycznych/, dostęp z dnia: 12.03.2018.

[6] Zaskórski P., Szwarc K., *Bezpieczeństwo zasobów informacyjnych determinantą informatycznych technologii zarządzania*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki", nr 9, rok 7, 2013.

[7] Zawiła-Niedźwiecki J., *Dobre praktyki czy teoria zapewniania ciągłości działania*, Politechnika Warszawska, Instytut Organizacji Systemów Produkcyjnych 2012.

[8] Ziemba E., Obłąk I., *Informatyczne wsparcie procesów w administracji publicznej*, [w:] *Technologie informatyczne w administracji publicznej*, Zeszyt 33/2014, red. A. Kobyliński, A. Sobczaka, „Roczniki Kolegium Analiz Ekonomicznych SGH", Warszawa 2014.

Statutory law

[1] Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r., DzU 2007 nr 89, poz. 590.

[2] Ocena ryzyka na potrzeby zarządzania kryzysowego. Raport o zagrożeniach bezpieczeństwa narodowego, RCB, Warszawa 2013.

Web pages

[1] https://encyklopedia.pwn.pl/haslo/;398219, dostęp z dnia: 10.03.2018.

[2] http://rcb.gov.pl/ksiega-dobrych-praktyk-w-zakresie-zarzadzania-ciagloscia-dzialania/, dostęp z dnia: 10.03.2018.

[3] http://www.gazetaprawna.pl/artykuly/977803,specjalisci-o-ciaglosci-dzialania-administracji-w-sytuacjach-kryzysowych.html, dostęp z dnia: 6.01.2018.

[4] http://www.politechnika.lublin.pl/dydaktyka/pliki/wyk/PSK_IMUZ/PSK_IMUZ_W5_lato2007.pdf, dostęp z dnia: 10.03.2018.

[5] https://www.up.lublin.pl/files/pracownicy/polityka_bezpieczenstwa_teleinformatycznego.pdf, dostęp z dnia: 2.03.2018.

[6] http://macierze-netapp.pl/technologie/rodzaje-raid.html, dostęp z dnia: 10.03.2018.

[7] https://dyski.cdrinfo.pl/artykuly/raid-konfiguracja-macierzy-dyskowych/strona2.php, dostęp z dnia: 10.03.2018.

[8] http://www.komputerswiat.pl/artykuly/redakcyjne/2016/11/wszystko-o-backupie.aspx, dostęp z dnia: 10.03.2018.

[9] http://www.ae.krakow.pl/~wiluszt/WSEI/SEMINARIA/wsei-2006-trynka-bezpieczenstwo-ro.pdf, dostęp z dnia: 10.03.2018.

[10] http://www.pszw.edu.pl/images/publikacje/t014_pszw_2008_zajdel_michalcewicz_-_analiza_zabezpieczen_systemow_informatycznych.pdf, dostęp z dnia: 10.03.2018.

[11] http://www.isok.gov.pl/pl/rzadowe-centrum-bezpieczenstwa-rcb, dostęp z dnia: 05.03.2018.

[12] https://rcb.gov.pl/wydzial-informatyki-i-lacznosci/, dostęp z dnia: 5.03.2018.

[13] https://rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/, dostęp z dnia: 12.03.2018.

[14] https://www.pbsg.pl/ciaglosc-dzialania-systemow-informatycznych/, dostęp z dnia: 10.03.2018.

WPŁYW NIEZAWODNOŚCI ORAZ CIĄGŁOŚCI DZIAŁAŃ NA SYSTEMY INFORMATYCZNE ZARZĄDZANIA KRYZYSOWEGO

Abstrakt. Obecnie ogromny wpływ na funkcjonowanie administracji publicznej mają systemy informatyczne. Są one niezbędne podczas zarządzania procesami i świadczenia usług publicznych. W dużym stopniu są one narażone na ataki cybernetyczne ze strony innych krajów, np. Rosji. Mówi się, że na całym świecie może dochodzić do ok. 1000 ataków co godzinę. To utrudnia albo uniemożliwia pracę systemom, które zapewniają sprawne funkcjonowanie państwa. Szczególnie ważny dla naszego bezpieczeństwa jest system zarządzania kryzysowego, który pozwala przeciwdziałać zagrożeniom i usuwać skutki ewentualnych katastrof. Jego nieodłączną częścią są niezawodne systemy informatyczne, które wchodzą w skład infrastruktury krytycznej. Dąży się zatem do zapewniania ciągłości działania systemu, ponieważ tylko wtedy możemy skutecznie zapobiegać sytuacjom kryzysowym. Elementem sprawnego działania administracji publicznej są niezawodne systemy informatyczne zarządzania kryzysowego. Po wystąpieniu sytuacji kryzysowych ogromna ilość informacji jest magazynowana i przetwarzana. Aby ułatwić zarządzanie informacją, tworzone są nowe narzędzia, które są wsparciem w podejmowaniu decyzji. Jednym z nich są Zintegrowane Systemy Informatyczne Zarządzania, dzięki którym możliwe jest zapobieganie kryzysom na skalę kraju. Działają one za pomocą wirtualnych technologii sieciowych przy wsparciu m.in. sztucznej inteligencji.

Słowa kluczowe: nowe technologie, informatyczne systemy bezpieczeństwa, zarządzanie kryzysowe, cyberprzestrzeń.