SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2020
ORGANIZATION AND MANAGEMENT SERIES NO. 145

INFORMATION SECURITY MANAGEMENT IN THE GLOBAL WORLD OF THE 21ST CENTURY

Piotr MAŚLOCH[1], Piotr GÓRNY[2*]

[1] Faculty of Management and Command, War Studies University, Poland; p.masloch@akademia.mil.pl
[2] Faculty of Management and Command, War Studies University, Poland; p.gorny@akademia.mil.pl
* Correspondence author

Purpose: The article attempts to determine what contemporary globalization is and what opportunities and threats this process creates (in terms of global threats to enterprise information systems).
Design/methodology/approach: The management of information security and counteracting cyber-attacks is an important aspect of the functioning of enterprises in the 21st century. In this sense, this article will analyse the threats resulting from the dynamic development of information technology, based on the results of research conducted on a sample of Polish enterprises.
Findings: This publication is an attempt to identify the basic threats resulting from the fact that the organization operates in a digitized global reality.
Research limitations/implications: It seems that the threats mentioned in the article will be gaining momentum and will be evaluated in the unpredictable today direction.
Social implications: The 21st century brought a completely new look at the processes of globalization and management of a modern enterprise. It turns out that information has become the basic tool of competitive struggle in the global market. For this reason, the management of information security and counteracting cyber-attacks is an important aspect of the functioning of enterprises in the 21st century.
Originality/value: The article addresses current problems of cyberspace security in the context of globalization. It can be useful for company managers as well as for conducting research in this field.

Keywords: management, global economy, information security, cyber-attacks, globalization.

Category of the paper: Literature review**.**

1. Introduction

The article "Information security management in the global world of the 21st century" is an attempt to show correlation relationships between the competitiveness of modern enterprises and their information security (cybersecurity). It should also be emphasized that broadly

understood competitiveness and security have been embedded in the realities of the impact of modern globalization processes on their functioning and development. The analyses of literature and research carried out in this study based on a sample of Polish enterprises aimed at identifying contemporary threats (cyber-threats) and presenting the importance and significance of these problems, so important for building a competitive advantage of enterprises operating in a dynamically changing global environment.

From a methodological point of view, two research methods were implemented: the first, theoretical one, based on the analysis of available literature and other studies on the issues discussed. The second one, having an empirical dimension, the essence of which consisted in analysing the research (reports) previously carried out, which in turn allowed to formulate specific conclusions and assumptions. As a result of the conducted analyses, it was possible to identify what factors do and will pose a threat to the information security (cybersecurity) of modern enterprises. The whole consideration is summarized by the presentation of the most important cyber-attacks on enterprises recorded in 1970-2016. Such a procedure was not accidental – the intended purpose of the authors is to indicate how great the threat is the information theft and increasingly common hacker attacks. In the belief of the authors, along with the development of more and more modern information technologies, the global world of the 21st century will be increasingly exposed to these phenomena.

2. Literature review

2.1. A new dimension of globalization. The role of information in the 21st century

Creating the basis of market economy in the countries of Central and Eastern Europe in the 1990s was associated with the establishment of a new social consensus, according to the requirements of the market economy organized around private ownership of capital. One of the important factors influencing and shaping the developing market economies in the former socialist countries was the globalization process. Globalization of the end of the 20th century, however differently defined, was based on the assumptions of peaceful coexistence of states and entire economies, based on market action on the grounds of free competition. Today, in retrospect, these idealistic assumptions turned out to be wrong. It is worth emphasizing at the moment that at the beginning of the 21st century, the threat of military conflict in the classical sense is less and less often discussed, and increasingly the internal security of the state is treated as, among others, economic security, internal security or cyber security. This should be kept in mind, because the diversity of global connections, including those based on new technologies, determines the essence of building the competitive advantage of individual countries. The end of the 20th and the beginning of the 21st century brought far-reaching changes on a global scale,

and in particular the emergence of many economic crises that significantly changed the balance of power in the world. To a lesser extent, these changes concerned military phenomena, although they also made themselves known, but in a larger dimension they appeared in the form of uncontrolled changes of a demographic nature, especially migration, to a scale unprecedented since World War II (Maśloch, 2016), terrorist threats and problems related to cyber security and access to information.

As A. Chmiel notes, rapid technological progress, which has been observed since the 1950s, caused a significant reduction in the costs of obtaining, processing and storing information. According to the theory of A. Tofler, we can now talk about a progressive information revolution, which is another stage of social development after the agrarian and industrial revolution. The stage of the information revolution will therefore be characterized by (Chmiel, 2017):

- Development of the services sector.
- Decentralization of management systems.
- Departure from mass production towards production adapted to individual needs.
- Declining share of the importance of access to natural resources.

The features of the information era presented above confirm that in the 21st century the key development factors are information and knowledge resources in the organization.

A similar opinion is expressed by W. Szymański stating that the critical problems of modern organizations will include (Szymański, 2008):

The ability to use access to the local market (to its demand and supply, capital, technical progress and innovation);

The ability to adapt to increasing uncertainty. Uncertainty in this case expresses a lack of information and knowledge, and therefore, the reduction of uncertainty depends to a large extent on overcoming the information barrier;

The tendency to introduce new products and innovations. Moreover, this ability must be associated with the ability of responsible, decisive and early destruction of the "old";

The ability to accumulate financial resources necessary to implement leading innovations.

Each decision-maker should have a well-organized information system for collecting, developing, storing, updating, restoring, processing and sharing data in accordance with the needs and requirements of users, necessary for the management staff to make decisions and for management (Górny, 2004).

The information **I** gathered and collected in such an information system can be treated as a “raw material” for the “production” of decisions **D**, which are the purpose of the decision system **T(I)** (fig. 1). Among the input information constituting the raw material, there should be information about:

- state of the object the decision concerns **(S)**,
- the decision-maker’s requirements and value system **(W)**,
- limitations and environmental conditions **(O)**.

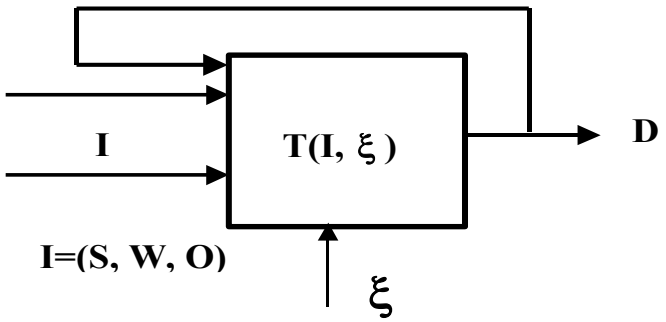


Figure 1. Information in the decision-making process.

The better the raw material, the more thoroughly processed, the better the product. The value of both of them is ultimately determined by the timeliness of delivery. However, the best decision (product) will be useless if it is developed too late – perhaps the need has already been satisfied in another, less satisfactory way or even the environmental conditions have changed so that it has already lost its relevance. Also, even the best input information for decision analysis, when delivered with a delay, will not be included in the decision-making process and as a result we will receive a decision (product) of inferior quality. The result will be unsatisfactory for the decision-maker both in the first and in the second situation.

At the same time, one should be aware that the decision-making process is not lacking disruptions. Therefore, the quality of decisions will also be influenced by the resilience of the decision-making system T to the disturbances ξ resulting from the variability of the environment or the variability of the object being the subject of decision-making. In today's reality, the system's resistance to all kinds of cyberspace threats also plays an important role.

As can be seen from the above, the basic stimulators of the enterprise development in the contemporary, globalized world are information, access and their management as well as information security, including cyber security.

2.2. Information security – information security model

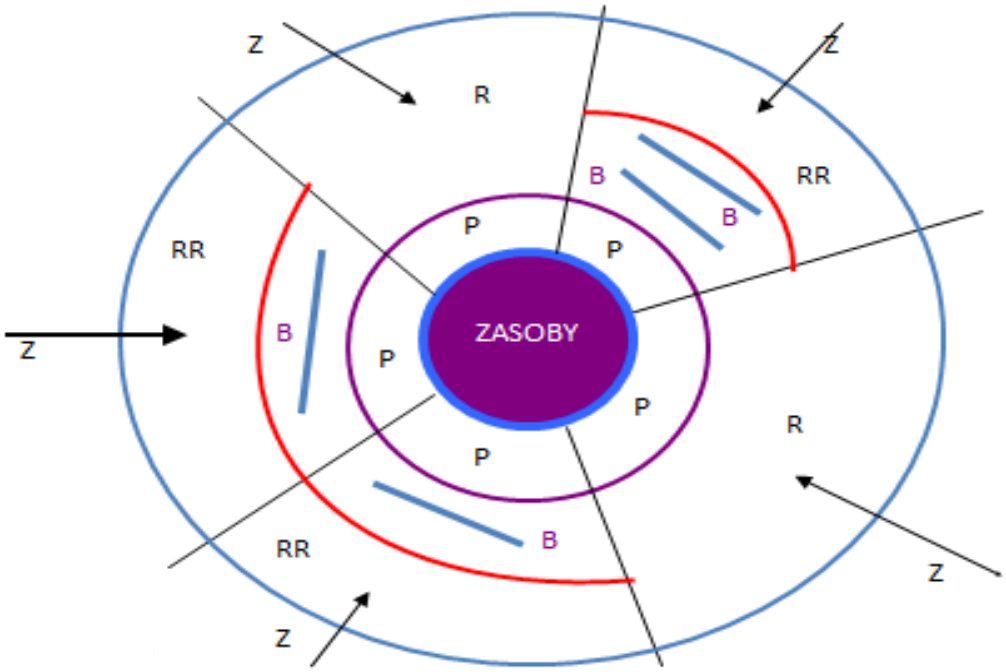
The concept of *information security* was introduced in the second half of the 20th century, but this does not mean that information as a security factor was of no importance before and was not perceived. Reliable, consistent, accurate and, at the same time, up-to-date information has always been and is important in making decisions, both those of a business as well as military and defence nature (Aleksandrowicz, 2016).

In the literature on the subject, the definition of state information security is most commonly found, but it can nevertheless be transported to the level of information security of each economic entity. It is worth paying attention to the model of P. Bączek, who proposes a layered (structural) model of information security, where the core is formed by techniques and information technologies surrounded by the following areas: social, ethical, cultural, scientific,

political, security and defence. Each of the areas of human life generates a different type of threats, characterized by its own specificity and at the same time capable of affecting the state of national security separately. At the same time, each of these spheres forms a separate subsystem of national information security, which must be secured in two ways: through universal solutions that apply to all layers and through solutions specific to each area. Threats to information security are of a trans-sectoral nature (Bączek, 2005). From a practical point of view, information security can be understood as protection of information against unwanted (accidental or conscious) disclosure, modification, destruction or disabling of its processing. With intellectual development and polytechnization of life progresses, information began to gain more and more values.

In the global world of the 21st century, the cyberspace that serves to transmit, process and store information is the natural sphere of information struggle. The essence of cyberspace is the use of information in the digitized form (Aleksandrowicz, 2016). Systems supporting information management are important assets of each institution. Ensuring an adequate level of information security is necessary to maintain market position, financial liquidity, meet legal requirements or maintain the image of the institution. Cyber security is therefore a problem that has to be considered in many aspects. The aim of cyber security policy is to present activities related to planning and management of IT security systems, as well as to present the roles and responsibilities of the organization's employees in this area. Responsibility applies to people managing the security of information systems whose main task is to design the system, its delivery and implementation, as well as usage of IT systems in a given organization. In addition to those responsible for the security of IT systems, these tasks should also be carried out by persons directly operating the given IT system.

Numerous information security models can be found in the literature, however, the model developed by international experts in the ISO standard is transparent and reflects this problem well. It is recommended that the implementation of the necessary security of each IT system should be executed on the basis of the security plan of that system (Górny, Krawiec, 2016). Raising general awareness of IT security systems, although often neglected, is an important factor affecting the effectiveness of security. The standardized information security model is shown in fig. 2.



P – susceptibility, B – security, R – risk, RR – residual risk, Z – threats.

Figure 2. General information security model.

Essential elements of this model include susceptibility and residual risk. Susceptibility is the weakness of assets or security, which can be used by a threat. The residual risk is the risk arising after dealing with risk and may contain unidentified and preserved risks.

A threat is a potential cause of an unwanted event that can cause harm in the system or organization. Generally, threats can be divided into human-dependent: intentional (U), accidental (P) and independent (N). IT systems are exposed to threats originating from many sources, both external and internal. Threats are becoming more and more sophisticated and cause significant losses in the material and non-material dimension. In order to ensure the desired safety level, it is necessary to properly identify these threats. The threat identification process should include these stages:

1. finding areas in which the object may be exposed to danger,
2. establishing sources, recognizing and classifying them,
3. anticipating the consequences and results of their occurrence.

In addition, identification should be carried out taking into account human and systemic or organizational factors.

Cyber security minimizes the risk for doing business and protects critical infrastructure, therefore it is important for both the public and commercial sectors. The basis for cyber security should be security procedures, supported by technical means.

2.3. Information security analysis on the example of Polish enterprises

The analysis of the level of cyber security on the example of Polish enterprises was carried out on the basis of the report from 2018 entitled: *Cyber-roulette in Polish. Why do companies count on luck in the fight against cybercriminals?* The report was prepared on the basis of a survey of 127 Polish experts dealing with IT and information security. The survey was conducted in autumn 2017 using the online survey method. The selected, most important research results presented in the report have been adequately presented in figures 3-5 (Maśloch, 2018).

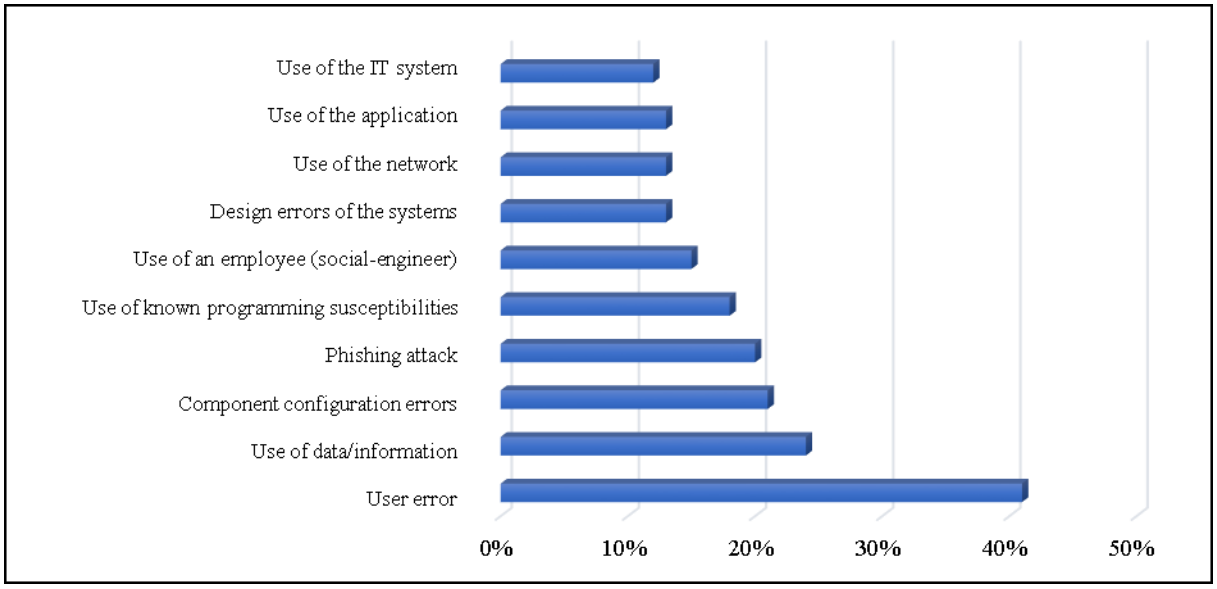


Figure 3. Causes of information security breach.

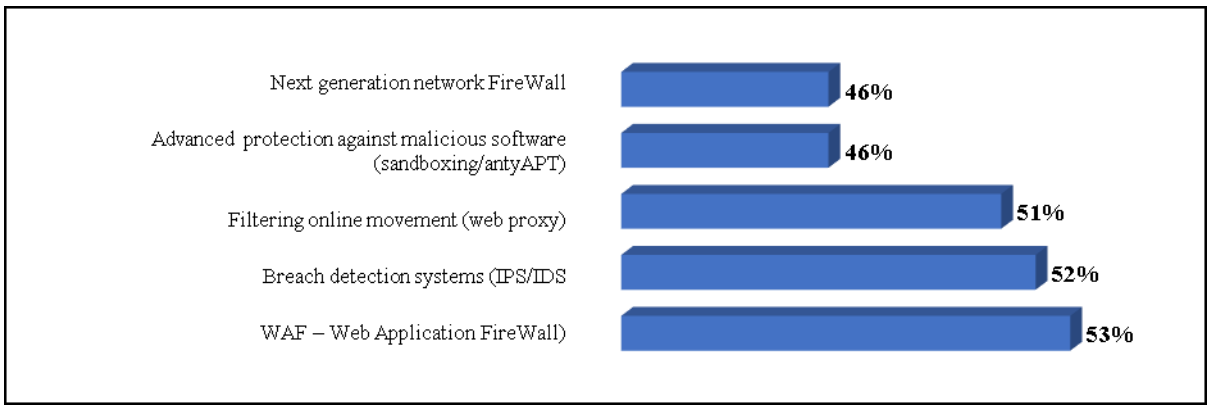


Figure 4. Types of implemented security measures.

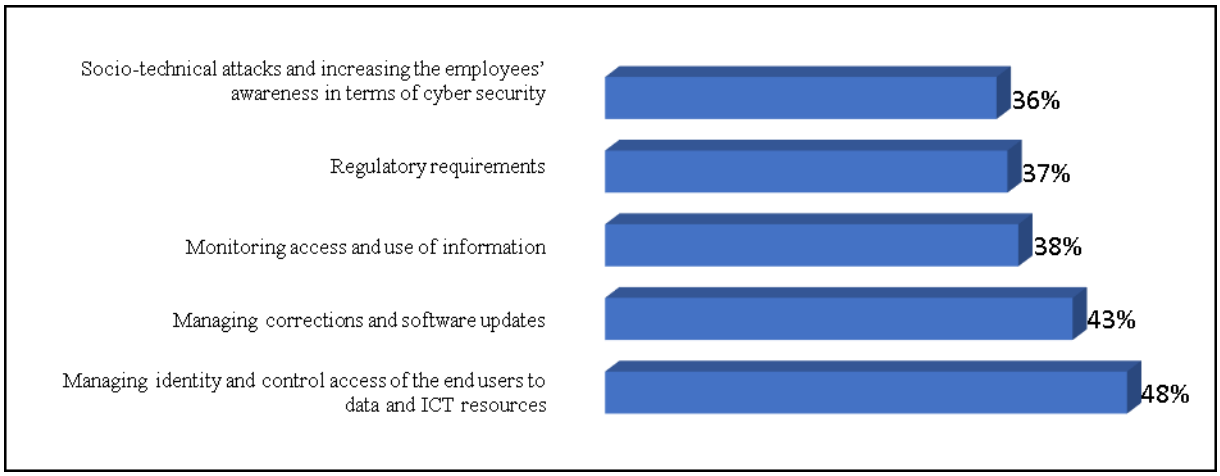


Figure 5. Challenges for information security.

According to the analysis of the obtained research results, 65% of companies indicated that incidents within which information security or IT systems were breached were detected within 12 months. However, not all incidents have been identified and included in the reports. The fact that 33% of surveyed companies indicated that the main source of incidents and threats was the immediate environment, i.e. current employees (13% of former employees, 6% of current service providers, consultants/contractors, 4% of clients, 2% of former service providers and suppliers) can be worrying.

As for the types of cyber-attacks and their start resulting from this, 21% of companies indicated that the systems were infected with ransomware malware. Considering the downtime in business, this was indicated by 15% of the surveyed companies, of which 40% (47% in 2016) of incidents were related to over a 3-hour break (12% - from 3 to 8 hours and from 9 to 24 hours, 15% - more than one day).

In order to present a full analysis regarding the increase of threats in the area of cyber security, table 1 presents selected types of cyber-attacks in the world in 1962-2017 (Górny, Krawiec, & Maśloch, 2017).

Table 1.
Examples of cyber-attacks in the world in 1962-2017

Year	crisis situation	cause
1962	Mariner 1 rocket going off course, which resulted in its destruction.	The "-" sign has not been moved to the control application.
1983	The computers of the USSR defence system showed the start of 5 ballistic missiles.	Erroneous interpretation of the reflection of sunlight on clouds in the USA.
1996	Ariane 5 rocket going off course, which resulted in its destruction.	Moving the software of the Ariane 4 rocket, which resulted in the maladjustment of the speed of the rocket.
1997	The NORAD system detected the attack of 2020 USSR missiles.	Sending random bits of information to the system.
2001	10 od 13 DNS (Domain Name Server) servers were shut down.	DoS (Denial of Service) types of attacks.

Cont. table 1.

2004	During the construction of the A-380 airplane, the aircraft equipment was not adjusted to the body of the aircraft, which resulted in a loss of about 5 billion euro and a delay of several months.	The CAT -CATIA program was used in the production of the aircraft in two versions 4 and 5 (Toulouse, Hamburg), two different operating systems (UNIX, WINDOWS) and programming languages (Fortran, C++) were used.
2007	3 of 6 attacked DNS servers were shut down.	DoS type of attacks, but the attack was limited after the introduction of the ANYCAST technology.
2008	Airbus SPAINAIR plane crash, which killed 154 people.	Incorrect positioning of the flaps during the take-off of the aircraft, caused by the introduction of malicious software during the servicing of the aircraft.
2008	B-2 Spirit (~ 1,3 billion $) crashed during the start from the Guam base.	No calibration of the sensors.
2010	First attack on critical infrastructure – taking over industrial processes at the nuclear power plant in Iran.	Taking control of the SCADA (Supervisory Control And Data Acquisition) system by the Stuxnet malicious program.
2012	Attack on the government websites in Poland with their immobilization for a certain period as a protest against the signing of ACTA agreements.	DDoS (Distributed Denial of Service) types of attack carried out by the Anonymous group.
2014	150 Ukrainian websites were blocked, NATO website and American security agencies websites.	DDoS type of attack.
2014/2015	Attack on 22,1 million users in the USA, data theft of 1.1 million people.	Hacker attack.
2015	Security breach of the Patriot missile launcher (Turkey).	Hacker attack.
2015	Immobilization of the power plant in Ivano-Frankivsk (Ukraine).	Hacker attack.
2016	Attack on smart buildings – failure of the heating and water supply system for the building – Lappeenranta (Finlandia).	Hacker attack.
2017	Attack on the NHS (National Health Service) hospital network – immobilization of the patient registration system (United Kingdom).	Attack using ransomware (WannaCry).
2017	Stopping the Nissan (Sanderland) and Renault (Great Britain) car production.	Hacker attack.
2017	Attack on 55 speed cameras in Melbourne (Australia).	Attack using ransomware (WannaCry).
2017	Attack on the network of nuclear power plants in the USA.	Attack using ransomware (Petya).

3. Methodology

The methodology used in the article was based on two basic elements: the first one, theoretical, in which the literature on the discussed issues was reviewed – the aim of such a review was to summarize and systematize existing knowledge. The second part is empirical – the analysis of cyber-threats for contemporary enterprises has been made on the basis of the already conducted research. The research procedure consists of two stages:

1. stage I, covering mainly literary studies in the field of information security, cyber security and globalization,
2. stage II, which deals with activities related to the analysis of the results of examinations already carried out, regarding the perception of cyber-threats by the surveyed enterprises.

The adopted methodology, based on a two-stage analysis of the problem, allowed to confirm the theoretical assumptions presented in the first stage by analysing the results of empirical research, which is part of the second study. It is also worth emphasizing that the catalogue of threats presented in table no. 1 and the frequency of their occurrence allow to think that we are and will be dealing with the problem of cyber security in the global world of the 21st century in the foreseeable future.

4. Conclusion

The globalizing world of the 21st century brings new challenges and creates completely different conditions for the functioning of modern enterprises. It is worth emphasizing that cyberspace, virtual world and information, which value is still growing, is one of the factors that create global reality. In this sense, this publication is an attempt to identify the basic threats resulting from the fact that the organization operates in a digitized global reality. This is all the more important because the development of modern technologies and cybertechnology is getting faster, covering still new areas of life, and thus the activities of individual enterprises. What is more, it seems that the threats mentioned in the article will be gaining momentum and will be evaluated in the unpredictable today direction.

References

1. Aleksandrowicz, T.R. (2016). *Podstawy walki informacyjnej*, 112-116.
2. Bączek, P. (2005). *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, 74-76.
3. Chmiel, A. (2017). Rewolucja informacyjna. In: *Przedsiębiorca w morzu informacji. Rola informacji w zarządzaniu zmianą gospodarczą. Raport końcowy*, 71.
4. Górny, P. (2004). *Elementy analizy decyzyjnej,* 26-27.
5. Górny, P., Krawiec, J. (2016). Cybersecurity – a system approach. *Scientific Notebooks AON, 2(18),* 77.
6. Górny, P., Krawiec, J., Maśloch, P. (2017). *Zagrożenia dla obronności i bezpieczeństwa państwa – wybrane problemy zarządzania,* 32.

7. Maśloch, P. (2016). *Globalization and contemporary challenges to security: illegal immigration. Scientific Notebooks AON, 2(1),* 85.
8. Maśloch, P. (2018). *Globalizacja a zarządzanie bezpieczeństwem współczesnych organizacji*, 140-143.
9. Szymański, W.(2008). Ewolucja przedsiębiorstw w warunkach globalizacji. In: A. Herman, K. Poznańska (eds.), *Przedsiębiorstwo wobec wyzwań globalnych*, 124.