SAFETY&DEFENSE
ISSN 2450-551X

Cybersecurity – One of the Greatest Challenges for Civil Aviation in the 21st Century

Małgorzata ŻMIGRODZKA

Military University of Aviation, Dęblin, Poland;
m.zmigrodzka@law.mil.pl, ORCID: 0000-0003-3896-0819

DOI: https://doi.org/10.37105/sd.73

Abstract

In every aspect of aviation's operations, from ground handling, aircraft designing and production, ensuring the continuity of flights, technical service, to air carriers, there is a possibility that cybercrime may occur. Ubiquitous computers, telephones, and internet carry the risk of various types of threats – from simple viruses, to personal data theft, to taking over of an aircraft by cybercriminals. The aim of the paper is to describe the main cyberthreats in the area of civil aviation. The theoretical analysis of the available source materials and empirical usage of security procedures in aviation organizations served as the main research methods that have been utilized in the analysis of the cybersecurity problem. The author's extensive professional experience in the aviation sector, especially in the field of quality and security, provided the possibility to verify and understand these vital problems for the aviation industry.

Keywords: cybersecurity, cyberthreat, risk, security, threat.

1. Introduction

Currently, a smartphone, laptop, or computer pose a threat on board an airplane. Cyber and mobile transformation, i.e., that what drives the revolution in aviation, constitutes a significant challenge. Growing automatization brings forth a larger risk of cyberattacks, because the more there are complex systems, the possibility that someone unauthorized, like hackers, can break in those systems is greater. Those systems can be used by criminal groups seeking political and financial benefits. For years, humanity saw the main threat in weapons. It seemed

that the systems and procedures were secured. However, at the beginning of the 21st century, in times of new technologies, we have to change the way of thinking. Most systems in aviation are automatized and based on the Global Navigation Satellite System (GNSS), especially on Global Positioning System (GPS), through which the autopilot of a flying aircraft may be interrupted, and the course or the destination changed (Compa, Rajchel, 2011).

2. Characteristics of cybercrime in the modern world

Technological capabilities of the 21st century galvanized the development of new criminal trends. These new technologies and phenomena should be understood and properly defined. Cyberspace is a complex notion and is usually linked to internal and external computer networks used for data transmission. Cyberspace is related to cybernetics, i.e., science dealing with the processes of control, transmission, and transformation of information. It consists of communication and information systems, links between them, and the relations with the users (BBN, 2015).

The language of the cyber world, which is difficult to understand, poses certain limitations for the average citizen. The data made available by not fully aware users of the information systems can be easily taken over and used for various purposes. Even the process of purchasing a plane ticket on the internet creates the opportunity for crime to be committed. A notion directly linked to cyberspace is cyberterrorism that takes place in it. It is a form of terrorism that came to being and was developed along with the technological development and globalization of information systems.

According to the 2019 KPMG report, 84% of the analyzed organizations see the largest threat in lone hackers (Fig. 1.). A real threat for the safety of aviation organizations is posed also by organized criminal or cyberterrorist groups, and disgruntled or bribed employees. Kids having access to various IT tools are able to break into booking systems, among other things. It is often done just for laughs.

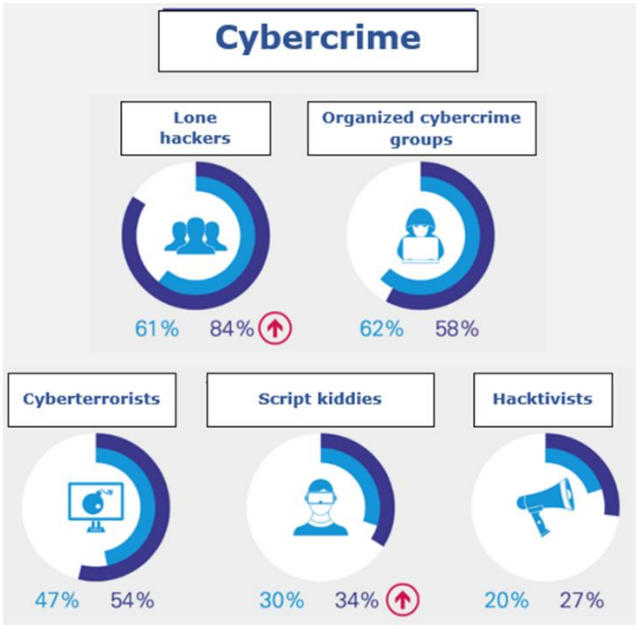

Figure 1. The perceived threat sources. Source: KPMG, 2019.

Taking into account the spectrum of the variety of possible attacks, it is necessary to describe a given phenomenon in more detail. Cyberterrorism is identified with unlawful actions targeting important communication and information systems in a way that the threat of carry them out enables reaching particular objectives or goals. People trained for these terrorist acts are not only schooled ideologically, but also have IT skills.

Figure 2. Visualization of interlinked systems in civil aviation that shows several potential paths of cyberattacks. Source: Vereinigung Cockpit, 2017.

Aviation is particularly vulnerable to all forms of terrorist attacks, and due to technological development to attacks in cyberspace as well. Among the possible threats, there are attacks with the use of malicious software, theft, modification or destruction of data, blocking access, and socio-technical attacks, i.a., phishing (Goodman, 2015). The aviation sector is mainly at risk due to cyberterrorist attacks, because it operates with a large amount of computer equipment, massive amount of data, which are transmitted every minute between electronic devices. Moreover, there is an arising necessity to rely on IT systems that are inevitable for the functioning of aviation today. Airports, airlines, navigation systems, flying an aircraft can become a target of a cyberattack. Even factories that manufacture components used for constructing airplanes can be attacked by cyberterrorist, which may lead to various, chiefly negative consequences for the whole aviation sector (ICAO, 2019).

3. The human factor and cybercrime

The internet is a generally accessible tool that offers its users many possibilities – from communication and acquiring knowledge, to enjoying shopping, medical, tourist, and other services. The growing threat of attacks that utilize shortcomings of the human mind make the human factor key in cybersecurity (Pisarek, Ščurek, 2017).

The 2019 ENISA report "Cybersecurity Culture Guidelines: Behavioral Aspects of Cybersecurity" informs that during last 25 years, actions meant to increase IT security have focused mainly on the technological security of systems and equipment. The role of the human being in the security systems was limited by procedures and sanctions (ENISA, 2019). Such an approach was responsible for the low level of social awareness regarding cyberattack prevention. However, it is well known that lack of education in that area generates a lack of understanding of the essence of cyberthreats. Therefore, enhancing the awareness of cyberspace is very important. Consequent implementation of secure global network services into everyday practices is equally vital. The need for deploying proper educational programs for employees from the private and public sectors is necessary because only through regular courses and training the state of cybersecurity may be improved.

In their research on cybersecurity, Mancuso (2014), Porctor and Chen (2015), Horowitz and Lucero (2016), and Heiges (2015) used a scenario which simulated the manipulation of the navigation system that presented false points on course (Gontar, et al., 2018). The main goal of the experiment was to learn what security requirements would be useful. The analysis of the human factor showed pilots' needs during a cyberattack, as well as their concerns regarding making inappropriate decisions. The biggest problem turned out to be the fact that during a cyberattack, pilots are uncertain (ICAO, 2015). In situations of technical malfunctions, pilots often act in accordance to procedures in order to solve them. In such a situation, pilots are also able to predict the behavior of the aircraft (e.g., if a hydraulic system is leaking). Pilots, acting in accordance with instructions, know that in a situation when hydraulic pressure is too low they would get a warning signalizing the malfunction. Moreover, pilots (depending on the aircraft) can get information from the aircraft system of how a particular malfunction will influence the aircraft's performance. Such situations are subject to training during simulator practices. It is worse during a cyberattack because pilots do not know whether the signals are trustworthy, or they can be unclear whether the system was attacked. Pilots, in such a situation, could be disoriented and not know if the problem could be solved by means of the established procedures. Following procedures, in such situations, can be

utilized by potential attackers to manipulate the pilots' behavior (Gontar, et al., 2018).

Potential cyberterrorist attacks aim at finding and making use of gaps and errors occurring in the security systems and shortcomings of human character that manifest itself in recklessness, laziness, or lack of imagination. The effects of cyberattacks may be the same as in the case of a terrorist attack – they have the potential of threatening of the lives of air transport users or their health, the destruction of airport infrastructure, or loss of important data for the aviation sector. Undoubtedly, the functioning of aviation is based on public trust, which can be irreversibly undermined by the occurrence of cyberattacks. This is why, , the aviation industry will face challenges to keep the public's trust in cyberspace in upcoming future. Solving these problems is crucial for the safe functioning of air transport.

4. Cybersecurity programs in Poland and the European Union

The European Union's actions regarding security in cyberspace are divided into two thematic areas. One of them is focused entirely on counteracting cyberattacks, while the second aims at maintaining the protection of critical infrastructure, IT critical infrastructure, and security of the network and information (Kańciak, 2013). According to that division between security and counteraction, the EU's programs and strategies have been prepared. There are, however, certain problems of a formal nature that have led to the lack of a common approach among the EU's institutions regarding those problems.

Security constitutes a fundamental air system and is a main goal of the EU's policy in the area of aviation and IT (Balcerzak, et al., 2019). Issues related to, i.a., the protection of critical infrastructure, personal data, and the environment are closely related to aviation security. Therefore, it is necessary that the EU's directives are implemented into national regulation frameworks. These documents are:

- Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection;
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union;
- Personal Data Protection Act of 10 May 2018;
- National Cybersecurity System Act of 5 July 2018;
- Ministry of Digitization Regulation of 10 September 2018 on the organizational and technological conditions for the entities providing services in the area of cybersecurity and internal organizational structures of the key services provides responsible for cybersecurity;
- Council of Ministers Regulation of 11 September 2018 regarding the list of key services and materiality thresholds of the effects of distorting events for providing key services;
- Ministry of Digitization Regulation of 20 September 2018 on the criteria of a breach of the security or integrity of the network or telecommunication services that have a significant impact on the operation of network or services;
- Ministry of Digitization Regulation of 20 September 2018 on a model form for the communication of information about security breaches or the integrity of telecommunications networks or services that have a significant impact on the operation of networks or services;
- Council of Ministers Regulation of 16 October 2018 on the documentation of cybersecurity of the IT systems used for providing key services.

The national cybersecurity policy framework of the Republic of Poland was established by a Council of Ministers' resolution. It has a direct bearing on government administration bodies. After being adopted, at

the initiative of the Council of Ministers, as the regulations of the national law, they, in an indirect way, affect other bodies of public administration. These regulations in particular refer to (Ministry of Digitization, 2017):

- The goals regarding computerized systems security;
- The main bodies engaged in implementation of the national framework of computerized systems security;
- The management framework facilitating the goals of national framework regarding computerized systems security;
- The need for preventing and reacting to incidents and recovery to the nominal state after disruption, including the rules of cooperation between the public and private sectors;
- The approach to risk assessment;
- The types of approaches to educational, information, and training programs regarding cybersecurity;
- The actions related to research and development plans in the scope of computerized systems security;
- The approach to international cooperation regarding cybersecurity.

Taking into account the development of the information society, electronic administration and digital economy, and the threats of cyberspace, the structures of the national protection of cyberspace have to be strengthened. Quickly changing methods of committing crimes require carrying our research in the area of counterfeiting cybercrimes, the results of which will provide support to law enforcement bodies (Żmigrodzka, 2011).

The body responsible for preventing hacker attacks is the Computer Security Incident Response Team (CSIRT GOV), whose key tasks focus on information exchange and knowledge sharing. The cyber emergency response center is a unit that monitors and reacts 24 hours a day and seven days a week.

Aviation is in the process of integration with the national system of cybersecurity, just as the power and financial sectors did previously. The main goal is to ensure the security of aviation operations in Poland by implementing all security procedures according to aviation law regulations.

Cybersecurity is not limited to IT but, above all, it consists in information. It is important not to marginalize even the smallest signs, because thanks to currently accessible technology, even a minor strange detail in the information or data may lead to significant losses, and thus it should be taken into account. Conclusions should be drawn from that information and then given over to other sectors and institutions because attacks can be multisectoral; they do not have to be direct.

5. Examples of risks and threats of cyberattacks in aviation

The whole development of aviation is based, to a considerable extent, on access to modern technologies, especially information technologies. All of the elements of the aviation sector should be aware of the risk that stems from using computer networks, and without which aviation activity could not exist. Recent incidents have shown that there is a growing interest in cyberspace among people who are willing to disrupt the functioning of aviation. In 2011, hackers were able to gain access to the radio frequencies used by British air traffic controllers, and give false information to the pilots and send a false signal about the danger. In the same year, a break into the internet network of one of the airlines was reported, in consequence of which the hackers gained access to confidential information about customers, their credit cards, flight plans, and data bases of that airline. The threat of cyberterrorism seems to be even more dangerous, because one just needs a computer with the internet access to carry out an attack. The cyberterrorists' knowledge and access they have to relatively cheap equipment makes them often feel that they are untraceable and unpunishable for creating real threat to the air transport users. Already at the level of providing software and operational systems

for the aviation sector, one should expect from the suppliers to provide updates on an ongoing basis, as well as to solve security related problems with the software they supply. Designing one piece of software for a particular company or institution from the aviation industry seems to be an ideal solution. It should not be available for other industries.

Enhancement of security may also consist in running applications as part of the so-called isolated areas, which limits undesirable software interactions. When it is accompanied by regularly updated anti-virus system, it decreases the risk of damages caused by cyberattacks. It should be obvious that the equipment dedicated to professional tasks cannot be used for private purposes. All data should be encrypted and properly secured. Especially sensitive systems should be cut off from the internet. A good example here is the fact of separation of the onboard entertainment system from other systems of the aircraft. Another important issue is data transfer, which ought to be performed only with the use of a secured, encrypted channel, and minimal internet connections. It should be noted that cyberattacks may go unnoticed even for a longer period of time. Therefore, there is a need for inspecting the accumulated data. Employees of various organizations of the aviation sector have to be aware that cybercrime threats may occur. Therefore, employers should organize specialized courses for their employees, which would include issues regarding how to increase employees' awareness of the security gaps in the data processing systems and how those systems could be attacked. The employees' skills should be also expanded by learning characteristic features of cyberattacks, so every one of them would be able to quickly recognize them and initiate limitation of its effects.

Higher risk related to cyberattacks in aviation occurs in the following areas (Żmigrodzka, 2011):

- Monitoring aircraft in airspace;
- Various IT software used by aircraft producers and operators;
- Activities related to operation of aircraft and support of people using the aircraft;
- Software that requires more secure programming so it would be ready to repulse every unpredictable cyberattack automatically;
- Securing against cyberattacks the equipment used for gathering and storage of important data;
- Management and control aiming at the deployment of proper security policies by the most important people in aviation organizations. Defining the process of risk management related to one's own organization and cooperating entities;
- Air traffic services that would profit from the implementation of monitoring systems and verifying the data they transmit;
- Access control with the use of the proper protocols and procedures, and limiting the access to particular sectors.

The main tasks of aviation organizations include, above all, the development and implementation of legal norms, procedures, and technological solutions enhancing security and development of aviation (Compa, 2017), as well as the following (Żmigrodzka, Kostur-Balcerzak, 2018):

- Licensing and Certifying;
- Carrying out audits, checks, and inspections;
- Carrying out scientific research, and development activities;
- Preparation of bills, normative documents, and manuals;
- Organizing courses and scientific conferences;
- Organizing civil-military cooperation at the national and international levels (Zajas, 2015).

An effective cybersecurity program should include using management structures based on international sectorial standards and guidelines in order to cover all necessary aspects.

One of the many issues related to prevention, and also to a certain degree, combating cyberterrorism is securing computerized

systems. EASA estimates that every year there are 1,000 cyberattacks on aviation systems globally (PA, 2018).

Despite the aviation industry lobby's belief that the systems aircraft are equipped with cannot be overtaken by hackers, researchers of the security market demonstrate the opposite. For example, at a conference in Greenberg (2013), Hugo Teso showed that he was able to manipulate the ACARS system used to address and report on aviation communication with the use of his smartphone running on Android. Ruben Santamarta, a security specialist, reveled in his research paper that he was able to take control of SATCOM radio telephones, which allowed him to conclude that the "current status of the products IOActive analyzed makes it almost impossible to guarantee the integrity of thousands of SATCOM devices" (Santamarta, 2014, p. 25).

In recent years, the number of cyberthreats related to airports has grown significantly, e.g.:

- Passport control systems at the departure terminals of Atatürk and Sabiha Gökçen airports in Istanbul were closed because of a cyberattack, which resulted in the passengers having to wait for hours in lines and light delays (2013) (PA, 2018);
- The resource planning system of a company managing airports in India was taken over, which resulted in losing personal employees data of 75 American airports. The break in was carried out by a organized hacker group financed by the state (2014) (PA, 2018);
- At Warsaw Frederic Chopin Airport there was a break in into the schedule planning system that caused grounding ten aircraft and delaying sever others. The hacker attack resulted in suspending flights that affected 1,500 passengers, and the teleinformation department was paralyzed for a few hours. Due to the breakdown, the Polish airlines LOT cancelled both domestic (from Warsaw to Kraków, Wrocław, Rzeszów, and Gdańsk) and international flights – to Dusseldorf, Hamburg, and Copenhagen (2015) (WP, 2015);
- Adata theft occurred at the Turkish Directorate General of Civil Aviation. The attack was discovered by a cybersecurity analyst working for Lockheed Martin, who noticed that hackers took control of two ICAO servers. Malicious software was installed on those servers and the software could be disseminated further by authorized government and aviation organizations employees. The hackers used the so-called water hole method, which gets its name from the way predators wait around their prey close to water holes. They used it to create the possibility of breaking into the server visited by their potential victims and install malware, which was ten downloaded by people logging in the ICAO server (2016) (Bounaoui, 2019).
- The Vietnam Airlines' webpage and information screens in Hanoi and Ho Chi Minh City airports were attacked by hackers, resulting in all systems connected to the internet being turned off, and all operations being carried out manually. The hackers obtained the data of 400,000 passengers (2016) (Bounaoui, 2019).
- There was an outbreak of ransomware that attacked systems, which resulted in the attacked organizations having to pay off hackers for getting data back. LATAM Airlines had their data decrypted by WannaCry and The Boryspil International Airport in Ukraine lost access to its systems because of ransomware called NotPetya. These cyberattacks did not target aviation, but caused a break in providing airport services (2017) (Bounaoui, 2019).
- The data from the transactions processed through a webpage and mobile application of a British carrier were taken over. The hackers gained access to credit cards numbers, their expiration dates, and CVV numbers. Such information make it possible for the cybercriminals to break into the customers' accounts and collect personal data. However, the passport and travel arrangements data were not targeted by the hackers (2018) (Górski, 2018).

6. Conclusions

In conclusion, threats to aviation security, especially frequent cyberattacks are one of the most important issues in the 21st century. Without proper training on the protection of IT infrastructure and making society aware of the danger, there is no possibility of ensuring security in aviation. The most common cases, as the research shows, are related to hackers' cyberattacks. Common strategy and policies to secure new technologies against undesirable access is key. Every computerized system connected to the internet or network can become a target, even aircrafts, which have been demonstrated in the paper. This is why, it is important to work out security procedures and common standards of using available, technologies created for aviation. Of course, while having regard to cultural differences, it has to be said, that it is a real challenge but, as it is the case with other security procedures, aviation security procedures have to be followed very restrictively.

References

1. Balcerzak, T., et al. (2019).Cybersecurity in civil aviation. In E. Dynia, and S. Kubas (Eds.), Bezpieczeństwo w międzynarodowym i krajowym prawie lotniczym i kosmicznym (pp.57-78). Rzeszów: Wydawnictwo Uniwersytetu Rzeszowskiego.
2. BBN [Biuro Bezpieczeństwa Narodowego] (2015). Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej z dnia 22 stycznia 2015 roku. Warszawa.
3. Bounaoui, S. (2019). Międzynarodowa Organizacja Lotnictwa Cywilnego padła ofiarą hakerów. RMF24, 08.03.2019. Retrieved from https://www.rmf24.pl/fakty/swiat/news-miedzynarodowa-organizacja-lotnictwa-cywilnego-padla-ofiara-,nId,2873380?fbclid=IwAR1qmuHK8XtIQm9nKywky0jOYARo1_2uMc_IwixJFkJoiY2QwxT6Ma5z_Cs, 10.04.2020.
4. Compa, T. (2017). Międzynarodowe organizacje lotnicze w systemie bezpieczeństwa transportu lotniczego. Dęblin: Wydawnictwo Wyższej Szkoły Oficerskiej Sił Powietrznych.
5. Compa, T., and Rajchel J. (2011). Podstawy nawigacji lotniczej. Dęblin: Wyższa Oficerska Szkoła Sił Powietrznych.
6. ENISA [European Union Agency for Network and Information Security] (2019). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. Retrieved from https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity, 19.03.2020.
7. Gontar P., et al. (2018). Are pilots prepared for a cyber-attack? A human factors approach to the experimental evaluation of pilots' behavior , Journal of Air Transport Management, 69, 26-37. DOI: https://doi.org/10.1016/j.jairtraman.2018.01.004.
8. Goodman, M. (2015). Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do about It. London: Corgi Books.
9. Górski, S. (2018). Atak hakerów na British Airways. Wyciekły dane kart kredytowych 380 tys. klientów. PCWorld, 07.09.2018. Retrieved from https://www.pcworld.pl/news/Atak-hakerow-na-British-Airways-Wyciekly-dane-kart-kredytowych-380-tys-klientow,410833.html.10.04.2020.
10. ICAO (2015). Podręcznik zarządzania bezpieczeństwem (SMM) (Doc. 9859 AN/474). Retrieved from http://edziennik.ulc.gov.pl/api/DU_ULC/2015/64/oryginal/Zalacznik1.pdf, 22.03.2020.
11. ICAO (2019). Security and Facilitation Strategic Objective: Aviation Cybersecurity Strategy. Retrieved from

https://www.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.EN.pdf, 18.04.2020.
12. Kańciak, A. (2013). Problematyka cyberprzestępczości w Unii Europejskiej. Przegląd Bezpieczeństwa Wewnętrznego, 8(5), 109-120.
13. KPMG (2019). Barometr cyberbezpieczeństwa: W obronie przed cyberatakami. Retrieved from https://assets.kpmg/content/dam/kpmg/pl/pdf/2019/04/pl-Raport-KPMG-Barometr-Cyberbezpieczenstwa-W-obronie-przed-cyberatakami.pdf, 22.04.2020.
14. Ministry of Digitization (2017). Krajowe ramy polityki cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017-2022. Warszawa: Ministerswo Cyfryzacji. Retrieved from https://www.gov.pl/documents/31305/0/krajowe_ramy_polityki_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/0bbc7a32-64df-b45e-b08c-dac59415f109, 12.04.2020.
15. PA (2018). Overcome the Silent Threat: Building Cyber Resilience in Airports. Retrieved from https://www.nsr-org.no/getfile.php/1310858-1532343127/Dokumenter/Eksterne%20publikasjoner/PA_Airport%20Cyber%20Security%20Report.pdf, 12.04.2020.
16. Pisarek, J., and Ščurek, R. (2017). Determination of the Human Factor in Air, Land and Marine Traffic. Saarbrücken: Lambert Academy Publishing.
17. Santamarta, R. (2014). SATCOM Terminals: Hacking by Air, Sea, and Land. IOActive Security Services. Retrieved from https://www.blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf, 10.04.2020.
18. Vereinigung Cockpit (2017). SafeSKY 2017. Retrieved from https://www.vcockpit.de/fileadmin/dokumente/presse/2017/Brosch%C3%BCre_SafeSKY2017_Onlineversion.pdf, 07.04.2020.
19. WP (2015). Systemy LOT narzędziem hakera. Wirtualna Polska, 29.09.2015. Retrieved from https://tech.wp.pl/systemy-lot-narzedziem-hakera-6034789869351553a, 10.04.2020.
20. Zajas, S. (2015). Międzynarodowe i krajowe organizacje lotnicze. Warszawa: Akademia Obrony Narodowej.
21. Żmigrodzka, M. (2011). Terroryzm powietrzny i środki jego zwalczania. In A. Kozera, et al. (Eds.), Polaków portret niedokończony: Studia z zakresu historii, prawa, politologii (pp. 360-373). Kraków: Wydawnictwo Naukowe Uniwersytetu Pedagogicznego w Krakowie.
22. Żmigrodzka, M., and Kostur-Balcerzak K. (2018). Measuring the Power of VR Education. In Transport Means 2018. Proceedings Of The 22nd International Scientific Conference: PART III (pp. 1459 -1463). Kaunas: Kaunas University of Technology.