Advances in Economics, Business and Management Research, volume 188
Proceedings of the International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research (BAMBEL 2021)

Aviation and the Cybersecurity Threats

Valeriia Filinovych [*1] [0000-0001-8824-615X], Zhengbing Hu [2]

[1] *National Aviation University, Kyiv, Ukraine*
[2] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine*
[*] *vvfilinovich@gmail.com*

ABSTRACT
The article points out the problem of legal regulation and ensuring cybersecurity in the aviation sector. This issue has acquired particular relevance in connection with the increasing level of development of information technologies in the aviation sector. The author analyses in detail the existing international standards and norms for ensuring aviation cybersecurity, substantiates the implementation of various initiatives and technologies on this matter. The study analyses the existing strategies and plans of international organizations in the aviation area and indicates the opinions of experts on the possibilities of solving the problems of cybercrimes in this area. To achieve the goals set for the study, the author actively uses dialectical, comparative, systemic, formal-logical, logical-normative, and statistical scientific methods. The article points out the need to harmonize national legislation with existing international regulations, and also provides recommendations for improving the level of cybersecurity in Ukraine and the world. The author also concludes that to achieve the goal of ensuring universal cybersecurity in the field of aviation, it is necessary to combine efforts not only by air carriers but also by all actors interested in maintaining the quality and safety of flights, as well as by national governments.

Keywords*: cybersecurity, cybercrime, aviation cybersecurity, safety of flights, critical information infrastructure.*

1. INTRODUCTION

The development of aviation led to the formation of a modern air transport system, which linked states and continents, provided an opportunity for a high-quality living for many social groups in hard-to-reach regions of the planet. Air transport has so organically entered our life that we can no longer imagine our existence without flights. Therefore, the slightest obstacle to the functioning of the air sphere immediately affects the lives of millions of people.

For the aviation sector of Ukraine, 2018 has become a landmark year: the passenger traffic of airports in the country for the first time exceeded the mark of 20 million and amounted to 20.55 million, which is 25% more than a year earlier. This growth ensured, first of all, the arrival of serious world low-cost airlines on the Ukrainian aviation market. But this factor also had negative consequences. Indeed, with the increase in passenger traffic, the risks for aviation safety in the country have also increased.

It is worth mentioning that in 2016-2017, Ukraine encountered powerful cyberattacks, then for some time, the work of many organizations, including critical transport infrastructure, was blocked. So, many Ukrainians remember how at the main airport of the country, Boryspil, on June 27, 2017, information on arrivals and departures on the information table was manually updated by the organization's employees, and many flights were delayed. Then the hacker attack also affected other air gates of the country (including the Odessa airport), some financial organizations, and other enterprises whose activities are key to the country's economy [1]. And this is only a small part of the problems that the so-called NotPetya computer virus has brought to our country.

The government of the state drew the right conclusions and in 2018 began to implement a national cybersecurity strategy. After all, we finally, like most of the world, realized that cyber threats are really dangerous. And the role of cybersecurity cannot be underestimated.

2. RESEARCH METHODS

The methodological basis of the paper is a set of universally recognized scientific cognition methods, in

particular the systematic method, thanks to which the author was able to establish the conceptual categories of cybersecurity in aviation and identify its place in the general security system of the aviation sector. Other research methods were also involved, which made it possible to provide a comprehensive analysis of threats in the field of aviation cybersecurity and cybersecurity itself.

The study was based on the dialectical method of scientific knowledge of the phenomenon of aviation cybersecurity in its relations and development. The author of the study also used such methods as a logical-normative method (to analyze and clarify the problematic issues of cybersecurity in aviation); formal-logical (for the purpose of analysis and expand the conceptual apparatus); comparative (to compare various approaches and methods to ensure cybersecurity in world practice); the methods of analysis and synthesis, and the synergistic method (which gave the author the opportunity to comprehensively analyze the problematic aspects of the incorporation of international norms of the cybersecurity regulation system into the national legislation of countries). The modeling method provided the development of recommendations for advancing legislation in terms of strengthening the cybersecurity in the aviation sphere.

3. PURPOSE OF THE PAPER

The purpose of the paper is to determine the concept and role of cybersecurity in the aviation sector, to identify deficiencies in its provision and legal regulation, and to formulate proposals aimed at improving standards and legislation to ensure the proper level of aviation cybersecurity.

4. OBJECT AND SUBJECT

The object of the study is relations arising concerning aviation security and cybersecurity in particular. The subject matter of the study is cybersecurity in the aviation sector.

4.1. The Concept of Cybersecurity and its Implications for the Aviation Sector

Digitalization in the air transport industry has enabled the relevant entities to provide better services to their customers. At the same time, as it became clear, the level of exposure to threats, especially cyberattacks, also increased.

Based on the foregoing, it is worth noting the key concepts and categories that the author of this scientific work will operate in the process of analyzing and presenting the material.

To begin with, it is important to determine the understanding of the term information security. This concept can be understood from several points of view. So, if we turn to ISO/IEC 27000 (2012), a range of international standards, including ones on information security, issued collectively by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), then by information security, one should understand the preservation of confidentiality, uprightness, and availability of information. In some cases, other properties such as authenticity, accountability, irrefutability, and reliability may be involved.

Y. Cherdantseva and J. Hilton understand this term as a branch of knowledge and professional activity, which exists in direct dependence on the development and implementation of protection mechanisms of all available types for storing data within and outside the perimeter of the structure, as well as directly information systems in which such threat-free data is created, stored and the like. At the same time, these types of information storage include both technical and legal, organizational, and others [2, p. 5].

As for the domestic legislation of Ukraine, according to the Law on the Basic Principles for the Development of the Information Society in 2007-15, information security is a state of protection of the vital interests of both a person and society and the state as a whole. In such a situation, the harm by providing incomplete, inaccurate, and untimely information is prevented in every possible way. In addition to providing the specified "negative" information to the corresponding malicious actions, this regulatory act also includes the negative information impact and the corresponding consequences of the use of information technology, unauthorized distribution, use and violation of confidentiality, accessibility, the integrity of information.

That is, by the information security of Ukraine, we mean the corresponding state of security of the information space of our state, while special operations and acts of external aggression with information connotations, unauthorized access, and theft of information through the use of special technical means, cybercrime and similar destructive actions do not cause tangible damage to the interests of the country [3, p. 124; 4]. Thus, we can say that the information security [5, 6] of the state is a set of effective mechanisms and measures of state bodies authorized to take appropriate actions in the information sphere, and their purpose is to protect the national security of the state (in our case, Ukraine).

The concept of information security is inextricably linked with the concept of cybersecurity [7, 8]. World practice knows several concepts of the latter, there is no single generally accepted one. Scientists have their own opinion on this matter. Thus, according to D. Schatz, R. Bashrow, and J. Wall, cybersecurity is the approach and actions associated with protection risk control processes that institutions and governments adhere to protect the confidentiality, probity, and availability of data and

assets used in cyberspace. The notion includes guidelines, strategies, and compilations of protection measures, technologies, tools, and training to provide the best protection for the state of the cyber asset and users [9].

M. Bezkorovainy and A. Tatuzov are sure that cybersecurity is a set of conditions under which all components of cyberspace are protected from the maximum possible number of threats and impacts with undesirable consequences [10, p. 25].

The abovementioned concept can also be defined as the state of security of cyberspace and the ability to prevent a cyber-attack in such a space (according to NIST SP 800-53 Rev. 4).

Thus, it is worth pointing out that not all information security issues are related to the notion of "cybersecurity". After all, there are systems (let's return to the topic of Aviation), isolated from the networks, and included in the technological circuit of air traffic control. That is why ensuring data security in them must be successfully harmonized with the information security fundamentals of a higher-level system.

The constantly mentioned cyberspace can be defined as a global area in the information environment, which included information systems, interdependent networks of information infrastructure systems, telecommunications networks, and computer systems, and the like (according to NIST SP 800).

As M. Bezkorovainy points out, cyberspace is nothing more than a sphere of activity in the information space. And such a sphere was formed by a set of communication channels of the World Wide Web and the technological infrastructure responsible for their functioning, as well as the sphere of any forms of human activity carried out through the use of communication channels. [10, p. 24].

Why is cybersecurity so important and necessary? Think about it: we interact with computers and computer networks every day: we work, develop business, build relationships, buy goods, incl. air tickets. With such a heavy reliance on computers, ignoring the likelihood of cybercrime, including in aviation, is extremely risky. So, we should remember the case with the Chinese plane Comac C919. According to a report by experts from Crowdstrike, the Chinese Ministry of State Security instructed its employees to coordinate the actions of hackers to obtain special intellectual property and developments, as well as find insiders working in aviation and aerospace companies. All this was done to create a powerful air transport based on Chinese resources, without using external materials [11].

In 2016, cyber attackers from the APT ALF group got unauthorized access to a defense subcontractor's information system, according to a report by the Australian Cybersecurity Center. As a result, about 30 GB of data was stolen, which constituted a secret, about the F-35 fighter, the P-8 Poseidon anti-submarine aircraft, the C-130 Hercules military transport aircraft, the Joint Direct Attack Munition (JDAM) ammunition, and about several modern Australian warships. At the same time, this subcontractor had ITAR certification, but its information systems had significant "holes" [12].

It is also worth mentioning how British Airways was fined £ 183 million in 2018 for a data breach. Then cyber criminals stole about 500 thousand personal data of passengers. The crime was committed by using a fraudulent web resource. The criminals received information about user data, such as login and password, payment card details, full name, addresses, information from air tickets [13].

In the same 2018, the Hong Kong air carrier Cathay Pacific was also subjected to a cyber-attack, as a result of which the personal data of 9.4 million people "leaked". This was information such as name, nationality, date of birth, email addresses, physical address, phone numbers, part of the passport data. According to representatives of the airline, not a single passenger profile was available in full, and hackers were unable to obtain customer passwords. As for payment cards, the cybercriminals received the data of 430 of them, while 403 had expired [14]. And there are many similar examples.

4.2. Solutions for cybersecurity issues in the aviation sector

The problem of aviation cybersecurity forced the governments of many countries, as well as international organizations, to make every effort to create the appropriate conditions for ensuring security in this area. So, of course, in this regard, we would like to mention IATA and ICAO.

It is safe to say that IATA is actively implementing all kinds of initiatives to improve and increase the level of cybersecurity in the aviation sector by producing various standards and regulative provisions and reducing technological gaps in every possible way.

IATA Media Days recently took place in Geneva, during which Nick Karen, Senior Vice President of IATA, shared his concerns about the current digital threats to aviation. According to him, with the advent of connected aircraft, cybersecurity ceased to be an on the ground issue. The specialist expressed confidence that due to the ability to easily "detect" the digital location of the aircraft, there were too many problems concerning the security of data transmission both onboard the aircraft (that is, when the crew communicates with the "ground"), and for the networks used for such a transfer. Karen also pointed out that hackers can break into the communication equipment of the passenger domain on

board the air transport, and, thus, they will gain access to the really important flight systems [15].

ICAO (hereinafter - Organization) is taking even more significant action to support cybersecurity in aviation. Last year, a special event, ICAO's 40th Assembly, was held at the headquarters of the International Civil Aviation Organization (Montreal), during which the Assembly Resolution A40-10 on cybersecurity in civil aviation was adopted, which declared the need to jointly address this problem and thus urged all countries to help implement the ICAO Cybersecurity Strategy. That is, the main idea of the Resolution is to organize cooperation between not only states but airlines and governments and to develop joint policies to ensure a holistic approach to aviation cybersecurity [16].

During this event, a representative of the Embry – Riddle Aeronautical University (ERAU) announced the participation of the university in the ICAO TRAINAIR PLUS Program and the implementation of the course “Fundamentals of Cybersecurity for Aviation". The course aims to train aviation professionals in identifying existing and potential cyber threats so that these participants can more effectively and quickly respond to such problems. Thus, the specified training will help ensure the safety of air travel for passengers around the world. The first recipients of new knowledge will be representatives of civil aviation regulatory bodies, civil airlines, and airports [17].

At the above-mentioned 40th Session of the Assembly, a specific ICAO Cybersecurity Strategy for the air transport sector was approved. This strategy aims to protect both passengers and the entire civil aviation sector from cyber threats affecting the safety of flights and the safety of the air transport system. Also, among its goals is the preservation and improvement of the quality of flight safety while maintaining the continuity of air traffic. The strategy is also intended to ensure consistency of actions for assuring cybersecurity between government agencies, which will help to effectively manage cybersecurity risk factors.

To achieve this, a group of principles and methods of a special mechanism will be applied, which includes seven key components, namely: cooperation between countries and organizations, the exchange of important data between these entities, the development of effective legislation, the introduction of a transparent cyber policy, joint planning of reactionary actions in case of incidents and emergencies; the formation of a culture of cybersecurity in parallel with the training of real professionals in this area.

The strategy highlights the importance of recognizing cybersecurity as a global aviation concern. It also provides countries with a conceptual vision of the sector being considered resilient to cyber-attacks and constantly evolving. The 40th Session participants readily endorsed the Strategy, recognizing it as the first of its kind to reflect key objectives for information data exchange and improve coordination across agencies.

Also, during the event, the representatives of the participating States asked the Organization leadership to do everything possible to achieve the advanced global goal of reducing to zero the number of fatal accidents in the aviation sector over the next decade. To achieve this, it is necessary to develop and implement new initiatives and plans for the provision of mutual assistance, effective strategic planning, as well as increasing professional potential.

The 2019 Global Aviation Safety Oversight System is an example of this initiative. This GASOS system will contribute to the expansion of cooperation in the field of aviation safety and at the same time will help to improve the situation on this issue in different countries.

The ever-expanding Technical Cooperation Program within Organization is also worth mentioning. During the 40th session, representatives of the civil aviation authorities of the participating countries, to expand technical cooperation and compliance with the standards of the Organization, held bilateral meetings and signed various agreements on the issue.

This program aims to strengthen government safety oversight. It also involves the conduct of investigations into accidents and emergencies in aviation. It is an evaluation program for Safety Oversight Organizations (SOOs) and Aircraft Accident Investigation Organizations (AIOs). Thus, the first does not explicitly include private organizations, nor does the second act as an intergovernmental regional organization.

Initially, ICAO wants to assess the level of training and the ability of SOOs and AIOs to perform certain aviation security functions. The Organization, conducting this assessment, publishes a list of SOOs and AIOs with a list of activities available to them in the GASOS directory, thereby helping the Member States to quickly find an institution to support and assist.

To make it easier for countries to ensure aviation security, ICAO supports regional mechanisms for mutual assistance and cooperation, including through the founding of local oversight organizations - the so-called RSOOs. Such entities help bring together individual Members' attempts at the regional level to provide greater safety oversight opportunities for Members. But many countries still do not comply with such conditions, as a result of which the GASOS program was introduced.

The recognition of each SOO or AIO now takes place in four stages:

1. Applying for and preliminary assessment. After the future SOO voluntarily applies for an application that includes the functions of the entity and basic information

about it, the Organization conducts a preliminary assessment to determine the sufficiency of the specified data. Following that, the request is accepted or denied, or the candidate is notified about the need to amend the document.

2. Self-assessment by the candidate followed by an on-site assessment by the Organization. A team of qualified GASOS specialists will be on-site for the evaluation. It will review the documentation, self-assessment outcomes, and evidence base.

3. On-site assessment. This group, together with the leader, will develop an on-site assessment plan, collect evidence, and present the results. The latter will just indicate whether the SOO / AIO meets the qualification requirements.

4. Summary and acceptance. The evaluation team will produce a draft report on it. The applicant will be able to give their comments. After all the specified SOO or AIO, GASOS will be recognized, which will be indicated in the GASOS directory [18].

Also, during the 40th Session of the Assembly, the implementation of the Global Aviation Security Plan, also known as GASeP, was approved, with more than 160 countries participating. The Plan aims to meet the needs of countries in particular, and the aviation industry in general, to lead efforts to improve safety in the aviation sector. This should be done through various internationally agreed actions and measures.

Thus, GASeP should help the Organization and its stakeholders to improve the effectiveness of aviation security at the global level. The Plan under consideration is intended to unite the international community and to encourage participants to take effective action on the issue of aviation security. At the same time, it is especially emphasized that the threats and risks that negatively affect the civil aviation sector are actively and continuously developing.

The activities of GASeP members are intended to help achieve five priority outcomes: raising awareness of aviation security risks and timely response to them; the development of a culture of such security with the simultaneous development of human potential; improvement of the technological base; improving the quality of supervision and control in this sector; widespread cooperation and mutual support [19].

A total of 94 GASeP Objectives have been documented, together with 32 actions under the 5 identified key results.

Let's return to the issue of ensuring security (both physical and cybersecurity) at critical infrastructure facilities. There is no definition of such a concept in ICAO documents, but a general explanation is provided. Thus, the Organization more often uses the term “vulnerable point”, meaning by it any object at the airport, or related to it, which, if damaged, will significantly disrupt the functioning of the “air gate”. Accordingly, such vulnerable points should be considered air transport control points, communication facilities, radio navigation aids, power equipment, and similar units both at the airport itself and outside it. Accordingly, such facilities should be provided with an adequate level of protection, including in the field of cybersecurity [20].

The organization has also developed general guidelines for the protection of sensitive data to ensure aviation security. The objects of their functioning are flight safety data. Accordingly, the circle of persons who have access to such information should be limited to those who need such data in the performance of their work duties. The so-called “need to know” principle operates here, that is, the possession of the specified individuals the right to access such information. Protective measures to ensure the safety of confidential information on aviation security issues should be taken in the event of identification, classification, reception, storage, enlightenment, distribution, or deletion of such data. There is a requirement that persons authorized to access confidential information sign a "nondisclosure agreement" before they are allowed access to this data.

ICAO also requires that every time such information is exchanged between countries, the latter clearly identify the information as confidential and communicate any specific safeguard requirements when it is transferred to other countries [20].

Thus, we see that the issue of aviation cybersecurity, taking into account the increasing development of information technology, is at the peak of popularity today both for specific countries and at the international level.

From the above, it becomes clear that the global aviation industry is taking many steps to improve its defensive position. SITA's 2018 AIR TRANSPORT IT Trends Insights report underlines that airlines and airports in many countries spend most of their investments in cybersecurity, with more than 95% of aviation market players planning to invest in major cybersecurity programs or similar research in the coming years. Unfortunately, only a little more than 30% of aeronautical organizations are confident that they are already able to deal with the cyber threats and risks of their occurrence [21].

According to the report, on average, air carriers spend approximately 7% of the total annual budget on information technology. This is in comparison with 10%, which are spent by the airports. Thus, aviation cybersecurity today is not getting the investment it needs, with costs amounting to 9%. This data reflects the growing importance of protecting databases and systems from illicit access. It should be noted that 73% of those surveyed cite compliance with regulatory requirements

and the regulation of the protection of personal databases as the most important goals and areas of work. This should be understood as the most important driver of investment in security over the past three years [21].

As R. Petrova says, the issue of cybersecurity forces the players of the aviation sector to face problems that are typical for other industries. Among other things, this is a lack of finance and material resources, as well as the professional skills of the staff. The scientist believes that the biggest obstacle to introducing the latest cyber developments in aviation is the lack of resources and the retention of qualified personnel specializing in resisting cyber-attacks. Accordingly, the main priority of the aviation industry today is to build a good base in IT security, as an essential component of protection against cyber-attacks [22].

Today there is a huge array of guides, recommendations, and instructions that are used by foreign players in the aviation market. These include, for example, RTCA DO-178B - a guide for assessing the safety and quality of software. It requires onboard air transport systems to be segregated and not interfere with the flight control process. Concerning encryption in the aviation sector, ISO / IEC 27002 is used. But Ukraine, and most of the world, is in no hurry to apply these documents in their practice.

Aviation experts agree that cyber threats pose a real threat to aviation today. This is primarily since modern air transport is being equipped with more and more sophisticated equipment, making it even more dependent on digital systems, which are often the target of cybercriminals' attacks. That is why Ukraine, like most states, should bring the issue of aviation cybersecurity to a qualitatively new level of study and assistance.

5. CONCLUSION

Today cybersecurity is one of the key issues in the aviation sector. Airlines and other organizations operating in this area are actively interacting and implementing various methods and technologies to ensure a sufficient level of security, both physical and virtual (digital).

For most countries in the world, the air transport sector is a part of the critical infrastructure of the state. Therefore, many governments are also concerned about the implementation of new standards and regulations to address risks in cyberspace. Along with them, industry organizations (ACI, IATA and others) develop relevant initiatives.

It is safe to say that today cyber-threats in the field of air transport are real and generally recognized. Therefore, both individual organizations and entire states are actively cooperating with the aim of mutual education, information and protection in the area under consideration. The exchange of information on security threats through various symposia and conferences, the organization of special centers for cyber threats (for example, SITA CCTC) and not only - all this is designed to ensure prompt notification of members of interested groups.

The industry has an integrated nature, accordingly, the approach to security should be aviation-oriented, namely, it includes assessing and defining business processes and assets of aviation organizations (for example, airports), which will help to highlight the really important and paramount tasks and nuances. But at the same time, one should not forget about the exchange of the obtained results, which will help ensure their higher accuracy.

The world community is faced with the need to develop a system of coordinated measures and a special decision-making procedure for ensuring the protection of the global aviation industry system from cyber-attacks. It is important not only to implement such actions but also to learn how to successfully combine them with periodic acts to protect the components of aviation cyberspace from external influences.

Mandatory, in our opinion, is the application of ICAO recommended practices, as well as harmonization of the national regulatory framework with international principles and standards in the field of cybersecurity. The resolution of cybersecurity issues in the civil aviation sector requires a concerted effort by all players in the aerospace sector. We can safely say that high-quality, effective, and reliable protection against cyberattacks in aviation should become a strategic priority for both the world community and the national security of each individual state.

REFERENCES

[1] Polityuk, P. and Auchard, E. Global cyber attack likely cover for malware installation in Ukraine: police official, Reuters, Series: Technology News (2017), available at: https://www.reuters.com/article/us-cyber-attack-ukraine/global-cyber-attack-likely-cover-for-malware-installation-in-ukraine-police-official-idUSKBN19K1WI

[2] Cherdantseva, Y. and Hilton, J. (2013), “Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals”, in: *Organizational, Legal, and Technological Dimensions of Information System Administrator*. Almeida F., Portela, I. (eds.). IGI Global Publishing, pp. 1-40, DOI: 10.4018/978-1-4666-4526-4.ch010

[3] Petryk, V. (2009), “The essence of information security of the state, society and person”, *Legal Journal*, vol. 5, pp. 122–127.

[4] Kovalchuk, T.I. Korystin, O.Y. and Sviridyuk, N.P. (2019), "Hybrid threats in the civil security sector in Ukraine", *Problems of Legality*, vol. 147, pp. 163-175, DOI: 10.21564/2414-990x.147.180550

[5] Zhengbing, Hu Yulia, Khokhlachova Viktoriia, Sydorenko and Ivan, Opirskyy (2017), "Method for Optimization of Information Security Systems Behavior under Conditions of Influences", *International Journal of Intelligent Systems and Applications*, vol. 9, no. 12, pp.46-58, DOI: 10.5815/ijisa.2017.12.05

[6] Pooja Yadav and Sangeeta Dhall (2020), "Comparative Analysis of Steganography Technique for Information Security", *International Journal of Mathematical Sciences and Computing*, vol. 6, no. 4, pp. 42-69, DOI: 10.5815/ijMSC.2020.04.05

[7] Pubudu K. Hitigala Kaluarachchilage, Champike Attanayake, Sasith Rajasooriya and Chris P. Tsokos (2020), "An Analytical Approach to Assess and Compare the Vulnerability Risk of Operating Systems", *International Journal of Computer Network and Information Security*, vol. 12, no. 2, pp. 1-10, DOI: 10.5815/ijcnis.2020.02.01

[8] Volodymyr, Tolubko Viktor, Vyshnivskyi Vadym, Mukhin Halyna, Haidur Nadiia, Dovzhenko Oleh, Ilin and Volodymyr, Vasylenko (2018), "Method for Determination of Cyber Threats Based on Machine Learning for Real-Time Information System", *International Journal of Intelligent Systems and Applications*, vol. 10, no. 8, pp.1 1-18, DOI: 10.5815/ijisa.2018.08.02

[9] Schatz, Daniel Bashroush, Rabih and Wall, Julie (2017), "Towards a More Representative Definition of Cyber Security", *Journal of Digital Forensics, Security and Law*, vol. 12, article 8, DOI: 10.15394/jdfsl.2017.1476

[10] Bezkorovainy, M. Tatuzov, A. "Approaches to the Definition of Cybersecurity" (2014), *Cybersecurity issues,* vol. 1, pp. 22-25, available at: https://cyberleninka.ru/article/n/kiberbezopasnost-podhody-k-opredeleniyu-ponyatiya/viewer

[11] Crowdstrike Huge Fan of Your Work Intelligence Report (2019), available at: https://www.crowdstrike.com/resources/wp-content/brochures/reports/huge-fan-of-your-work-intelligence-report.pdf

[12] Stilgherrian, B. Secret F-35, P-8, C-130 data stolen in Australian defence contractor hack, ZD Net (2017), available at: https://www.zdnet.com/article/secret-f-35-p-8-c-130-data-stolen-in-australian-defence-contractor-hack/

[13] Sweney, M. "BA faces £183m fine over passenger data breach. The Guardian" (2019), available at: https://www.theguardian.com/business/2019/jul/08/ba-fine-customer-data-breach-british-airways

[14] Horton, W. "Cathay Pacific Faulted for Data Breach, But Hackers' Objective Unclear" (2019), *Forbes, Series: Aerospace & Defense*, available at: https://www.forbes.com/sites/willhorton1/2019/06/06/cathay-pacific-faulted-for-data-breach-but-hackers-objective-unclear/#56ba698e7068

[15] Bailey, J. "Cybersecurity in aviation: Should we be worried?" (2019), *Get Connected*, available at: https://www.getconnected.aero/2019/12/cybersecurity-aviation/

[16] A40-10: Addressing Cybersecurity in Civil Aviation, ICAO (2019), available at: https://www.icao.int/cybersecurity/Documents/A40-10.pdf

[17] Aviation Cybersecurity Fundamentals - A New Course in the ICAO TRAINAIR PLUS Program (2019), available at: https://avianews.info/osnovy-kiberbezopasnosti-dlya-aviatsii-novyj-kurs-v-ramkah-programmy-ikao-trainair-plus/

[18] About: What is GASOS, ICAO (2019), available at: https://www.icao.int/safety/GASOS/Pages/About.aspx

[19] ICAO Global Aviation Security Plan (GASeP), ICAO (2019), available at: https://www.icao.int/Security/Pages/Global-Aviation-Security-Plan.aspx

[20] Protecting Critical Infrastructure Against Terrorist Attacks: A Compendium of Best Practices, INTERPOL (2018), available at: https://www.un.org/sc/ctc/wp-content/uploads/2019/07/RUS-compendium-final.pdf

[21] SITA Air Transport cybersecurity insights, ICAO, (2018), available at: https://www.icao.int/NACC/Documents/Meetings/2018/ CSEC/D12b-AirTransportCybersecurityInsights2018-SITA.pdf

[22] Petrova, R. (2020), "Legal Aspects of Ensuring Flight Safety under Cyber Threats: the Case of Civil Aviation", *Enforcement Monitoring*, vol. 1 (34), pp. 56-60, DOI: 10.21681/2226-0692-2020-1