

S. Ya. Lykhova,

Doctor of Law, Professor

ORCID ID: <https://orcid.org/0000-0003-4755-7474>

COMPUTER SAFETY OF AVIATION

National Aviation University

Liubomyra Huzara Avenue, 1, 03680, Kyiv, Ukraine

E-mail: sofia.lykhova@gmail.com

*The article is aimed to characterize the new profession in the aviation sector, namely the personal data protection officer. Currently, the National Aviation University is a pioneer in teaching the course «Prevention of Criminal Offenses in the Field of Computer Aviation Security», designed primarily for the second master's degree in higher education, specialty 262 «Law Enforcement». **Methods of research:** cognitive-analytical, system analysis, etc. At present, the vast majority of aviation businesses face many challenges in the field of data security. First of all, it is necessary to ensure the security of personal data, because the airline can process tens of millions of records of passengers during the day. Aircraft, crews and passengers on board should also be under cyber protection. Leaks or cyberattacks can have serious consequences. Therefore, at the present stage, the issue of cybersecurity of civil aviation has ceased to be the subject of attention only of IT professionals. **Discussion:** many airlines need to introduce the position of Data Protection Officer (DPO), the main purpose of which was to ensure the implementation of regulatory and organizational support of business processes related to the processing and protection of personal data. The purpose of this work is to analyze the main tasks facing the Data Protection Officer in the field of aviation and proposals to address these issues during the training of this specialist in the specialty 262 «Law Enforcement». The methodological basis of the study is the classical method of system-structural analysis. **Results:** the article concludes that the position of personal data protection officer belongs to the category of compliance specialists, and the main purpose of which was to ensure the implementation of functions of regulatory and organizational support of business processes related to the processing and protection of personal data. His or her work in airlines is characterized by complete independence from the executive body of the company - the decisions of the officer concerning the processing and protection of data have no right to influence any of the employees, including management. An officer may not be dismissed for decisions taken within his or her competence. The basic knowledge required to perform his/her production functions by a personal data protection officer is a thorough knowledge of international and international, in particular European, laws on personal data protection and the practice of their application.*

Key words: information protection; information security; civil aviation; cyber threat; compliance.

Problem statement and its topically. Currently, the National Aviation University is a pioneer in the teaching of the course "Prevention of criminal offenses in the field of aviation computer security", designed, first of all, for the second master's level of higher education, specialty 262 "Law enforcement activity".

Currently, the absolute majority of business entities in the aviation industry are faced with many

challenges in the field of security data. First of all, it is necessary to ensure the security of personal data, because the airline can process tens of millions of records about passengers during the day. Under cyber protection planes, crews and passengers must also be on board.

In the era of digitization, when most airline tickets are purchased online, the airline processes a large number of highly sensitive information - bank

data cards, passport numbers, phones, names and customer names, etc. A leak of such data or a cyber attack can have serious consequences. Therefore, at the current stage, the issue of ensuring cyber security of civil aviation has ceased to be a subject of attention only for IT specialists.

This is due to the fact that the data operated by the airline is in one way or another related to the personal data of customers, employees and other natural persons who provide the company services. After the introduction of the requirements of the new EU regulation 2016/679 on the protection of individuals with regard to the processing of personal data and the free movement of such data from 04.27.2016. In many airlines, it became necessary to introduce the position of data protection officer (DPO), the main purpose of which was to ensure the performance of functions of regulatory and organizational support of business processes related to the processing and protection of personal data.

Officers for the protection of personal data in modern conditions must understand both the technical component of ensuring cyber security issues, and possess knowledge of the regulatory provision of cyber security issues and personal data protection. On a practical level, their work is related to the thorough study of national, European and international regulatory acts and standards in the field of personal data protection and cyber security, as well as the development of internal company documents on the specified issues, as well as monitoring their implementation.

Analysis of recent research and publications.

The sphere of civil cyber security aviation is inherently interdisciplinary field of research. To one degree or another, O. Zolotar [1], T. Oleshko [7], A. Ilyenko [2], V. Kharchenko [9], O. Korchenko [4], Yu. Lisovska [6], N. Semchuk [8] and others paid attention to these issues.

The purpose of this paper is the analysis of the main tasks faced by the personal data protection officer in the field of aviation and proposals for solving the specified issues during the training of the specified specialist in specialty 262 "Law enforcement activities".

Main material. First of all, it is worth paying attention to certain technical aspects of cyber security in the field of civil aviation, which are neces-

sary for the formulation of further regulatory recommendations.

As noted by A. Ilyenko [2, 24–25]. Ukraine first experienced a cyber attack on computer systems and the central server of Boryspil and Kharkiv airports in June 2017, which led to aircraft service denials and flight delays. A few months later, in October 2017, flight departures from Odesa airport were delayed as a result of computer network hacking airport, which led to the loss of confidentiality of information. According to the experts of the European Aviation Safety Agency (EASA), during 2019, the world's aviation systems were exposed to cyber attacks up to 1,000 times every month. Thus, approaches to countering cyber attacks should be systematic, reliable and comprehensive, the aviation industry is one of the critical transport infrastructure of Ukraine. A safety program for the transmission of critical information in the relevant aircraft avionics systems should be developed for network and data protection, reliability, integrity and security. Effective security of the transmission of critical information in computer-integrated aviation systems is aimed at combat various threats and prevent them from entering or spreading in the aircraft avionics systems. The most common threats include: viruses, Trojan horses; hacker attacks; provoking pseudo-failures during the operation of various FIS and AA complexes when in fact the systems are in working condition; data interception and theft; activities and influence of hostile intelligence agents, etc. A successful attack can lead to complications in the operation of functional systems of the aircraft, the development of complications in flight conditions, and in the case of an increase in false data about flight conditions, to emergency and catastrophic situations. Threats can cause a wide variety of failures and failures, because aircraft avionics are very complex and saturated with complex computer networks [2, 35–36].

Civil aviation activities within the "land-to-air" and "air-to-air" channels, the issue of safe operation of such aviation systems is becoming increasingly acute. In fact, each flight takes place in a complex system of networks, which includes a number of components: 1) the ground computer network of the airport and airlines, 2) the on-board computer network of the aircraft, 3) the network of information

transmission between the communication methods of the control centers of airports and aircraft (AA) and air navigation systems for providing and controlling air traffic along the flight route.

Despite the fact that the risk of unauthorized interference exists in each of the systems, which can create significant problems for aviation security, the officer for the protection of personal data in the field of aviation is primarily responsible for compliance with regulatory requirements and internal regulations for the security of the ground computer network airport and airlines.

As T. Oleshko points out, growing globalization and the wide spread of data analysis technologies are radically changing the organization of airspace management and the air transport market in general. Over the past 10 years, high-tech solutions in civil aviation have made it possible to offer consumers new standards of flight safety, quality of service and comfort of air transportation [7, 43-46].

At the same time, along with the digitization of the flight process, the process of digitization of passenger service is underway. Digitization in the field of airline passenger service is one of the primary tasks aimed at modernizing management and creating a convenient and practical service system for customers. In the coming years, solutions aimed at increasing speed and passenger service quality. If now the registration of passengers is mainly carried out at the counters and takes an average of 1-1.5 minutes per person, then by 2030, using relevant services and mobile applications, a large part of passengers will go through the online registration procedure. The presence of special RFID tags and sensors will allow passengers to monitor the movement of luggage in real time. Airlines are also implementing effective IT solutions in the field of on-board passenger service. Developments aimed at improving the quality of service and improving service on board aircraft are already being actively used: prompt transfer of flight status information for the airline website; the information system for managing in-flight meal orders on airline flights; IT provision of the service of providing children's sets for children depending on their age categories [7, 43].

Leading airlines and large airports are actively implementing the Internet of Things technology,

connecting to it an increasing number of physical infrastructure elements and developing special navigation programs that analyze information from sensors about the location of objects. The Internet of Things is a set of physical objects connected to the Internet and equipped with sensors, from smartphones, tablets to cars and jet engines, which collect data and exchange them over a network, including local or wireless. At airports, technologies allow combining notification systems and monitoring the movement of all objects to make the stay of passengers more comfortable and safe, transferring data to their portable electronic devices (smartphones, tablets, etc.), which are important for navigation [7, 46].

A separate item is the electronic flight bag (EFB), which is essentially a tablet that the pilot takes with him on every flight, which contains a huge amount of information about the flight, the crew and the passengers on board the plane. Although convenient, EFBs pose a real risk to flight safety that airlines need to properly assess and control accordingly [5].

Understanding the technical part of the tasks facing the personal data protection officer, let's consider the practical aspects of his work. Currently, it is common to define the work tasks of the personal data protection officer. Such tasks are most often covered by the concept of compliance.

T. Kobeleva points out that the term "compliance" is borrowed from the English language (compliance - agreement, conformity, from the verb to comply - to answer) and characterizes an action in accordance with a request or indication; is currently the direction of professional activity. In practice, the concept of compliance is closely related to the management/control system in the organization, as well as the risks of non-compliance, non-compliance with the requirements of legislation, regulatory documents, rules and standards of supervisory bodies, industry associations and organizations, codes of conduct, etc. [3, 116-120].

In the aviation industry, a new interaction of interested parties has been formed, which actively assess the risks of data loss and cyber security risks, which is directly related to both the introduction of the latest technologies and the new regulatory acts in the field of personal data protection (GDPR).

Companies began to actively implement additional measures to ensure information security, in particular the security of personal data, which, of course, is directly related to cyber security [5].

Since the data protection officer is actually responsible for data privacy-compliance, which is directly related to cyber security, the expansion of the function and area of responsibility is currently relevant. In particular, it is important to constantly review and update internal acts regulating cyber security issues. The participation of this specialist is also required in the processes related to the remote work of the company's employees.

Additional expansion of functions will also take place in connection with the implementation of the requirements of the European Union regarding the protection of personal data in the process of joining the European Union.

It is worth touching on the organizational aspects of the personal data protection officer's work. According to open data, this person in airlines is characterized by complete independence from the company's executive body — none of the employees, including the management, have the right to influence the officer's decisions related to data processing and protection. An officer cannot be dismissed for decisions made within his competence [5].

Conclusion. Graduates of higher education at the master's level in the specialty 262 "Law enforcement activities" after listening to special courses on cyber security in the field of aviation can work as officers for the protection of personal data. This is due to the fact that the data operated by the airline are in one way or another related to the personal data of customers, employees and other natural persons who provide services to the company. After the introduction of the requirements of the new EU regulation 2016/679 on the protection of individuals with regard to the processing of personal data and the free movement of such data from 04.27.2016.

The position of personal data protection officer belongs to the category of compliance specialists, and the main purpose of his work is to ensure the performance of functions for regulatory and organizational support of business processes related to the processing and protection of personal data. His

work in airlines is characterized by complete independence from the executive body of the company - none of the employees, including the management, have the right to influence the officer's decisions related to data processing and protection. An officer cannot be dismissed for decisions made within his competence.

The main knowledge required for the performance of the personal data protection officer's duties is a thorough knowledge of laws and international, in particular European, issues of personal data protection and the practice of their application.

In the course of work, the personal data protection officer is responsible for the constant review and updating of internal acts regulating cyber security issues - both confidentiality agreements, trade secret protection agreements, and clauses regarding the processing of personal data regarding clients. The participation of this specialist is also required in the processes related to the remote work of the company's employees. Also among the tasks is the constant monitoring of the existing situations with the protection of personal data and taking measures against their violation.

Literature

1. Золотар О. Охорона інформації як напрям у інформаційній безпеці в складі безпеки цивільної авіації та її співвідношення із захистом інформації. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2009. № 1 (18). С. 23-31.

2. Ілленко А., Ілленко С., Кваша Д. Сучасний стан кібербезпеки цивільної авіації України та світу. *Кібербезпека: освіта, наука, техніка*. 2020. № 1 (9). С. 24-36. DOI: <https://doi.org/10.28925/2663-4023.2020.9.2436>

3. Кобелева Т. Сутність та визначення комплаєнс-ризиків. *Вісник Національного технічного університету «Харківський політехнічний інститут»*. Економічні науки. 2020. № 1. С. 116-212. DOI: <https://doi.org/10.20998/2519-4461.2020.1.116>

4. Корченко О., Бурячок В., Гнатюк С. Кібернетична безпека держави: характерні ознаки та проблемні аспекти. *Український науковий журнал інформаційної безпеки*. 2016. № 19 (1). С. 40-44.

5. Коваленко С. Особливості функції комплаєнс в авіаційній галузі. *Юридична газета online*. 2021. № 8 (738). URL: <https://yurgazeta.com/dumka-eksperta/osoblivosti-funkciyi-komplaens-v-aviaciyniygaluzi.html>

6. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. Київ: Видавничий дім «Кондор», 2019. 272 с.

7. Олешко Т.І., Попик Н.В., Бабич М.О. Цифровізація бізнес-процесів в цивільній авіації. *Економіка та держава*. 2021. № 4. С. 43-46. DOI: <https://doi.org/10.32702/2306?6806.2021.4.43>

8. Семчук Н.О., Тімуш Д.І. Якісні методи дослідження кримінального права: український та іноземний досвід. Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право». Київ: НАУ, 2020. № 4(57). С. 182–187. DOI: <https://doi.org/10.18372/2307-9061.57.15083>

9. Харченко В., Корченко О., Гнатюк С. Базова модель формування вимог до забезпечення кібербезпеки цивільної авіації. *Український науковий журнал інформаційної безпеки*. 2016. № 22(2). С. 150-155.

References

1. Zolotar O. Okhorona informatsii yak napriam u informatsiinii bezpetsi v skladi bezpeky tsyvilnoi aviatsii ta yii spivvidnoshennia iz zakhystom informatsii. *Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini*. 2009. № 1(18). P. 23-31.

2. Illienko A., Illienko S., Kvasha D. Suchasnyi stan kiberbezpeky tsyvilnoi aviatsii ukrainy ta svitu. *Kiberbezpeka: osvita, nauka, tekhnika*. 2020.

№ 1(9). P. 24–36. URL: <https://doi.org/10.28925/2663-4023.2020.9.2436>.

3. Kobielieva T. Sutnist ta vyznachennia komplaiens-ryzyku. *Visnyk Natsionalnoho tekhnichnoho universytetu «Kharkivskiy politekhnichnyi instytut» (ekonomichni nauky)*. 2020. № 1. URL: <https://doi.org/10.20998/2519-4461.2020.1.116>.

4. Korchenko O., Buriachok V., Hnatiuk S. Kibernetychna bezpeka derzhavy: kharakterni oznaky ta problemni aspekty. *Ukrainskyi naukovyi zhurnal informatsiinoi bezpeky*. 2016. № 19(1). P. 40–44.

5. Kovalenko S. Osoblyvosti funktsii komplaiens v aviatsiinii haluzi. *Yurydychna hazeta online*. 2021. № 8 (738). URL: <https://yurgazeta.com/dumka-eksperta/osoblivosti-funkciyi-komplaens-v-aviaciyniy-galuzi.html>.

6. Lisovska Yu.P. Kiberbezpeka: ryzyky ta zakhody: navch. posibnyk. Kyiv: Vydavnychiy dim «Kondor», 2019. 272 p.

7. Oleshko T.I., Popyk N.V., Babych M.O. Tsyfrovizatsiia biznes-protsesiv v tsyvilnii aviatsii. *Ekonomika ta derzhava*. 2021. № 4. P. 43–46. URL: <https://doi.org/10.32702/2306?6806.2021.4.43>.

8. Semchuk N.O., Timush D.I. Qualitative methods of criminal law research: Ukrainian and foreign experience. *Scientific works of National Aviation University. Series: Law Journal «Air and Space Law»*. 2020. № 4(57). URL: <https://doi.org/10.18372/2307-9061.57.15083>

9. Kharchenko V., Korchenko O., Hnatiuk S. Bazova model formuvannia vymoh do zabezpechennia kiberbezpeky tsyvilnoi aviatsii. *Ukrainskyi naukovyi zhurnal informatsiinoi bezpeky*. 2016. № 22(2). P. 150–155.

КОМП'ЮТЕРНА БЕЗПЕКА АВІАЦІЇ

Національний авіаційний університет
проспект Любомира Гузара, 1, 03680, Київ, Україна
E-mail: sofia.lykhova@gmail.com

Метою статті є характеристика нової професії в авіаційній сфері, а саме офіцер із захисту персональних даних. Наразі Національний авіаційний університет є піонером у викладанні курсу «Профілактика кримінальних правопорушень у сфері комп'ютерної авіаційної безпеки», призначеного, в першу чергу, для здобувачів вищої освіти другого (магістерського) рівня за спеціальністю 262 «Правоохоронна діяльність». **Методи дослідження:** пізнавально-аналітичний, системного аналізу тощо. В даний час переважна більшість авіаційних підприємств зустрічаються з багатьма проблемами в сфері безпеки даних. У першу чергу, необхідно забезпечити безпеку персональних даних, адже авіакомпанія може обробляти десятки мільйонів записів пасажирів протягом дня. Повітряні судна, екіпажі та пасажирів на борту також повинні перебувати під кіберзахистом. Витоки або кібератаки можуть мати серйозні наслідки. Тому на сучасному етапі питання кібербезпеки цивільної авіації перестало бути предметом уваги лише IT-фахівців.

Обговорення: багатьом авіакомпаніям необхідно ввести посаду фахівця з питань захисту даних (DPO), основною метою якої буде забезпечення здійснення нормативного та організаційного бізнес-процесів, пов'язаних з обробкою та захистом персональних даних. Метою даної роботи є аналіз основних завдань, що стоять перед співробітником з питань захисту даних в галузі авіації та пропозиції щодо вирішення цих питань під час підготовки такого фахівця за спеціальністю 262 «Правоохоронна діяльність». Методологічною основою дослідження є класичний метод системно-структурного аналізу. **Результати:** автор статті доходить висновку, що посада співробітника з питань захисту персональних даних належить до категорії спеціальних фахівців, і основною метою якої буде забезпечення реалізації функцій нормативно-правового та організаційного бізнес-процесів, пов'язаних з обробкою та захистом персональних даних. Його робота в авіакомпаніях характеризуватиметься повною незалежністю від виконавчого органу компанії – рішення посадової особи, що стосуватимуться обробки і захисту даних, і які не матимуть права впливати ні на кого зі співробітників, в тому числі й на керівництво. Посадова особа не може бути звільнена за рішення, прийняте в межах її компетенції. Базовими знаннями, необхідними для виконання своїх виробничих функцій співробітником з питань захисту персональних даних, є досконале знання міжнародних, зокрема європейських, законів про захист персональних даних та практики їх застосування.

Ключові слова: захист інформації; інформаційна безпека; цивільна авіація; кіберзагроза; відповідність.

Стаття надійшла до редакції 22.11.2022