Nikolay Shelukhin

Ivan Kharaberiush

Olga Gromova

DOI: https://doi.org/10.32353/acfs.4.2021.05
UDC 343.983:614.841

Nikolay Shelukhin,
Professor, Chair of Law and Public Administration, Mariupol State University, Doctor of Law, Professor, Mariupol, Ukraine
ORCID: https://orcid.org/0000-0002-3197-9659
Google Scholar: https://scholar.google.com.ua/citations?user=YLJ1-v4AAAAJ&hl=ru
Scopus: https://www.scopus.com/authid/detail.uri?authorId=57209683888
e-mail: shelukhin2004@inbox.ru.

Ivan Kharaberiush,
Professor, Chair of Law and Public Administration, Mariupol State University, Doctor of Law, Professor, Mariupol, Ukraine
ORCID: https://orcid.org/0000-0002-4968-5421
e-mail: hif52.04@gmail.com

Olga Gromova,
Independent researcher, Ph.D. in Law,
Vishnevoe, Ukraine
e-mail: hromova.o.n.2016@gmail.com

The Place of Cyber-Terrorism Countermeasures in the System of Criminological Security of Enterprises of the Aerospace Industry of Ukraine

Counteraction to cyberattacks on enterprises of the aerospace industry of Ukraine is considered within the framework of theories and institutions of criminological science. The place of cyber-terrorism counteraction in the system of criminological security of enterprises of the aerospace industry of Ukraine has been determined. The general characteristics of the elements of the system of criminological security of the enterprises of the aerospace industry in Ukraine are highlighted. It is emphasized that cyber-terrorism counteraction is the main component of the system of criminological security of enterprises of the aerospace industry in Ukraine. The concept of criminological security of aerospace enterprises is given, the system of this security and its components are disclosed.

Keywords: system of criminological security, countering cybercrime, aerospace industry, cyberattacks, victimological prevention.

Introduction

During total globalization, the global economic crisis and the spread of coronavirus infection, the challenges and threats faced by Ukraine and the entire world community are largely associated with the rapidly growing role of information and communication technologies. Their widespread use today is not only a guarantee of technological progress and the successful development of society, but also the reason for the high degree of human addiction to the security of the information and communication sphere. With the development of information and communication technologies, the methods of committing crimes in the field of high technologies are also developing. The commission of crimes using digital technologies is already an obvious fact, the number of these crimes has become widespread in recent years. These types of crime primarily include crime with the use of virtual assets (cryptocurrency), crime in the field of intellectual property, in the context of digital

© N. Shelukhin, I. Kharaberiush, O. Gromova, 2021

transformation, economic criminality, crime in the illegal circulation of narcotic drugs and psychotropic substances, extremism and terrorism[1].

In the 80s of the last century, exploring the tendencies of the transition of terrorism from the physical to the virtual world and the convergence of threats in this world, Barry Collin, senior researcher at the Institute for Security and Intelligence, proposed a new concept of "cyberterrorism"[2]. Currently, cyberterrorism is understood as a set of illegal actions in cyberspace that threaten the state security, individuals and society. The main goal of cyberterrorism is to influence the solution of social, economic and political problems[3].

The issues of countering cyberterrorism are discussed almost in all major international forums. The World Economic Forum 2018 report noted that cyberattacks have become more dangerous and widespread (occupying the third position in the ranking of the most probable threats to the national and global economy) and are comparable to fraud in a technological aspect[4]. Experts associate cyberattacks with such possible incidents: interruptions and even disabling of critical information infrastructure; errors and failures of financial mechanisms or institutions; terrorist attacks; various types of fraud, theft and misuse of data of individuals and/or legal entities, documents of commercial or government importance.

Some experts are inclined to believe that the energy and telecommunications industries and aviation control facilities are more susceptible to terrorist cyberattacks. Published documents highlight the importance of this issue: Pathways Towards a Cyber-Resilient Aviation Industry World Forum Report[5], International Civil Aviation Organization Cybersecurity Action Plan[6], ICAO Cybersecurity Strategy[7], decision of the 13th Air Navigation Conference "Improving the concept of cybersecurity in aviation" [8] etc.

Literature Review

A fairly large number of studies in various fields of science: natural, technical, social and public have been devoted to the issues of countering cyber-terrorist attacks on critical infrastructure facilities, including aviation. Scientists from various countries and schools were involved in developments in this area of knowledge. The most complete contribution to the socio-humanitarian block of research in the field of cyber-terrorism countermeasures against critical infrastructure objects was made by such scientists as: J. Allen, V. P. Babak, P. D. Bilenchuk, M. O. Belyaev, S. S. Boskholova, S. A. Gnatyuk, V. A. Golubev, A. A. Korchenko, J. McHugh, E. Metropoulos, V. O. Maximov, O. O. Mitrofanov, M. V. Shevchenko, S. V. Karpenko, A. Kh. Korch-

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Disclaimer

The funder had no role in the study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Contributors

The author contributed solely to the intellectual discussion underlying this paper, case-law exploration, writing and editing, and accept responsibility for the content and interpretation.

Declaration of Competing Interest

The author declare that they have no conflict of interest.

[1] E. g., Fighting against cybercrime: problems and prospects in Ukraine and the world / Andrii Borko, Vadym Nehodchenko, Olena Volobuieva, Ivan Kharaberiush, Yevheniia Lohvynenko // Journal of Legal, Ethical and Regulatory Issues. 2019. Vol. 22, Special Issue 2. Financial and legal regulation of electronic money circulation in developed countries / Semen Stetsenko, Olena Yu. Syniavska, Mykola L. Shelukhin, Serhii Lukash, Yevhen Barash // Journal of Legal, Ethical and Regulatory Issues. 2019. Vol. 22, Special Issue 2.

[2] Collin B. The Future of Cyberterrorism. Crime & Justice International Journal. 1997. № 13 (2). P. 15-18.

[3] Плотов В. И., Михайлов Д. М., Педанов В. А. Угрозы терроризма в условиях цифровой трансформации мира и пути защиты от них. Гуманитарные науки. Вестник Финансового университета. 2020; 10(1):14-20. DOI: 10.26794/2226-7867-2020-10-1-14-20

[4] World Economic Forum. URL: https://www.weforum.org/

[5] Пути к киберустойчивой авиационной отрасли. URL: https://www3.weforum.org/docs/WEF_Pathways_Cyber_Resilient_Aviation_2021.pdf

[6] План действий по обеспечению кибербезопасности Международной организации гражданской авиации, опубликовано 5 ноября 2020 года. URL: https://m.favt.gov.ru/public/materials//1/7/e/3/b/17e3bdfb0c48411080846e9b7116f8aa.PDF

[7] Стратегия ИКАО в области кибербезопасности, принято на ассамблеи 40 сессии ИКАО 25.06.2019 года. URL: https://www.icao.int/Meetings/a40/Documents/WP/wp_028_ru.pdf

[8] Совершенствование концепции кибербезопасности в авиации. Решение 13 Аэронавигационной конференции. Монреаль, Канада, 9–19 октября 2018 год. URL: https://www.icao.int/Meetings/anconf13/Documents/WP/wp_042_ru.pdf

Н. Л. Шелухин, И. Ф. Хараберюш, О. Н. Громова

МЕСТО КИБЕРТЕРРОРИСТИЧЕСКОГО ПРОТИВОДЕЙСТВИЯ В СИСТЕМЕ КРИМИНОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ АЭРОКОСМИЧЕСКОЙ ОТРАСЛИ УКРАИНЫ

Актуальность исследования: актуальность исследуемой проблемы обусловлена потребностью в рассмотрения противодействия кибератакам на предприятиях аэрокосмической отрасли Украины в рамках теорий и институтов криминологической науки.

Цель исследования: цель статьи заключается в уяснении места кибертеррористического противодействия в системе криминологической безопасности предприятий аэрокосмической отрасли Украины, выделении и общей характеристики элементов системы криминологической безопасности предприятий аэрокосмической отрасли Украины.

Методы исследования: ведущими общенаучными методами исследования данной проблемы являются анализ литературы по проблеме противодействия киберпреступности; классифицирование – уяснение элементов обеспечения криминологической безопасности предприятий аэрокосмической отрасли; аналогии; изучение и обобщения сведений.

Результаты исследования: в статье дано понятие криминологической безопасности предприятий аэрокосмической отрасли; раскрыта система этой безопасности и ее составляющие; уяснено, что кибертеррористическое противодействие является основной составляющей системы криминологической безопасности предприятий аэрокосмической отрасли Украины.

Практическая значимость: материалы данной статьи могут быть полезны для преподавателей криминологии высших учебных заведений, практических криминологов, работников предприятий аэрокосмической отрасли Украины, занимающихся противодействию киберпреступности.

Ключевые слова: система криминологической безопасности, противодействие киберпреступности, аэрокосмическая отрасль, кибератака, виктимологическая профилактика.

enko, A. Christie, O. V. Orlov, M. I. Panov, J. Pickel, J. Platt, E. V. Patsyra, H. O. Spitsyna, I. A. Tereykovskiy, V. P. Kharchenko, Yu. B. Chebotarenko, V. Yu. Shepitko, O. V. Shesler, N. E. Filipenko, V. Fiten, I. Ya. Friedman et al.

In recent years, new developments and opinions have appeared on the organization of preventive measures in the field of computer technology, priority areas of law enforcement, the process of reforming the regulatory framework for countering cyberterrorist attacks, and so on. In the development of the basic provisions on cyberterrorism countermeasures at critical infrastructure facilities, a number of monographic works have been published in recent years, these are, first of all: "Predictive modeling of computer virus epidemics", "International security, strategic stability and information technology", "Countering cyberterrorism in digital era ", "Cyberwar: the law and ethics of virtual conflicts", "Counterterrorism. Ethical issues", monographs-yearbooks "Information security in critical infrastructures" for 2017-2020[9] and others, which summarize the results of recent studies in various areas related to the safe and efficient operation of critical infrastructure facilities.

It should be emphasized once again that scientists and practitioners from all over the world are involved in the fight against cyberattacks (digital crime, cyber terrorism, cyber crime[10].

At the same time, despite a significant amount of doctrinal and practical researches in the field of countering cyberattacks on critical infrastructure facilities, the studies of the above scientists did not exhaust this problem, but, on the contrary, outlined a number of new theoretical and practical problems that require their solution. From the point of view of criminal law policy, the task of determining the place of cyber-terrorism countermeasures in the system of criminological security of enterprises in the aerospace industry of Ukraine has not been studied before, which determines the necessity and relevance of this work.

Main Content Presentation

a) The concept of criminological security of enterprises of the aerospace industry in Ukraine.

An analysis of the research of scientists-criminologists, their judgments about the concept, subjects, tasks and structure of modern criminology as a science indicates that at present, within the framework of the science of criminology, a large number of new theories and institutions have appeared,

[9] E. g., Прогностичне моделювання комп'ютерних вірусних епідемій: монографія / Шевченко В. Л., Нестеренко О. В., Нетесін І. Є., Шевченко А. В. Київ : УкрНЦ РІТ, 2019. 152 с.; Международная безопасность, стратегическая стабильность и информационные технологии / отв. ред. А. В. Загорский, Н. П. Ромашкина. М.: ИМЭМО РАН, 2020. 98 с.; Степанов О. Противодействие кибертерроризму в цифровую эпоху М. : Юрайт, 2021. 103 с.; Бегишев И. Р. Преступления в сфере обращения цифровой информации / И. Р. Бегишев, И. И. Бикеев – Казань: Изд-во «Познание» Казанского инновационного университета, 2020. 300 с.; Cyber War: Law and Ethics for Virtual Conflicts / Jens David Ohlin, Kevin Govern, and Claire Finkelstein, Oxford Scholarship Online, 2015. DOI: 10.1093/acprof:oso/9780198717492.001.0001; Counter-Terrorism. The Ethical Issues / Edited by Seumas Miller. Open access books. 2021, 224 p.

[10] E. g., Robert J. Bunker, Terrorism Futures: Evolving Technology and TTPS Use (Indianapolis, IN: Xlibris/A C/O Futures Pocketbook, 2020), 160 pp.; Gus Martin, Understanding Terrorism: Challenges, Perspectives, and Issues [7th Edition] (Los Angeles, CA: SAGE, 2021), 592 pp.; Douglas Pratt, Religion and Extremism: Rejecting Diversity (New York, NY: Bloomsbury Academic/An Imprint of Bloomsbury Publishing Plc., 2018), 208 pp.; Jez Littlewood, Lorne L. Dawson, and Sara K. Thompson (Eds.), Terrorism and Counter-Terrorism in Canada (Toronto, Canada: University of Toronto Press, 2020), 352 pp.; Горшенева И.А., Гольцева О.Ю. Особенности противодействия преступлениям кибертеррористической направленности (Зарубежный опыт) / Ирина Аркадьевна Горшенева, Ольга Юрьевна Гольцева //Криминологический журнал, 2019. -№3. – С.10-16; Назаров, В. Л. Международный опыт профилактики экстремизма : [учеб. пособие] / В. Л. Назаров, Е. В. Осипчукова. – Екатеринбург : Изд-во Урал. ун-та, 2015. – 248 с.; Экстремизм и терроризм в киберпространстве: угрозы миру и безопасности человечества: сборник статей по итогам III Всероссийской студенческой научнопрактической очно-заочной видеоконференции / под ред. В.А. Мазурова, М.А. Стародубцевой. – Барнаул: Изд-во Алт. ун-та, 2020. – 203 с.

which sometimes go far beyond the study of crime. Moreover, so far that anti-crime researches turn into research on the motives of crime - in the field of anthropology, etiology, social sphere, ecology, family relations, mass communications, medicine, sports, religion, etc. Due to the absence in criminology as the science of unambiguous definitions of the first row (concept, subject, tasks, structure), derivative definitions are also a subject of discussion[11]. One of these definitions is the concept of "criminological security". The concept of "criminological security" is essentially multi-vector, along with such fundamental concepts of criminology as: crime, delinquency, crime rate, etc. The concept of "criminological security" was formulated by legal scholars representing the Eastern school of law and introduced into circulation in the countries of the former USSR and Eastern Europe[12].

In modern criminology, there are several approaches to defining the concept of "criminological security". Initially, when this concept was introduced into scientific circulation, "criminological security" meant the security of the object of protection. So the founders of the introduction of the "criminological security" concept into scientific circulation: M.P. Kleymenov and A.V. Artyomov, M.M. Babaev, V.A. Pleshakov defined it as an objective state of protection of vital and other essential interests of the individual, society and the state from criminal encroachments and threats of such encroachments, as well as people's awareness of their security. Realizing at the same time that threats are criminal activity in all forms[13].

In our opinion, G.A. Avanesov explains the concept under study more logically and correctly. He believes that the concept of "criminological security" is identical with the set of measures to prevent criminal encroachments and this concept is understood as "the set of political, ideological, economic, socio-psychological, legal and other measures developed and implemented by the competent state and public structures, as well as citizens, to prevent criminal encroachments on the rights of the individual, society, state"[14].

Given the high degree of threats posed by the destabilization of the activities of the aerospace industry, based on and logically continuing the research by M.P. Kleymenova, A.V. Artyomova, M.M. Babaeva, G.A. Avanesov, we come to the conclusion that the criminological security of enterprises of the aerospace industry should be understood as the protection of these enterprises from threats aimed at destabilizing their activities by implementing a set of measures of a different nature: technical, political, ideological, economic, socio-psychological, legal, etc.

b) The system of criminological security of enterprises of the aerospace industry of Ukraine and its components.

In order to timely and properly respond to the criminological challenges of our time that threaten the security of enterprises in the aerospace industry in Ukraine, it is necessary to have a clear understanding of the system for ensuring the criminological security of these enterprises.

As mentioned above, the system for ensuring the criminological security of the aerospace industry is the set of measures used in the process of

М. Л. Шелухін, І. Ф. Хараберюш, О. М. Громова

МІСЦЕ КІБЕРТЕРОРИСТИЧНОЇ ПРОТИДІЇ В СИСТЕМІ КРИМІНОЛОГІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ АЕРОКОСМІЧНОЇ ГАЛУЗІ УКРАЇНИ

Актуальність дослідженя: актуальність досліджуваної проблеми зумовлена потребою в розгляді протидії кібератакам на підприємствах аерокосмічної галузі України в межах теорій та інститутів кримінологічної науки.

Мета дослідження: мета статті полягає в з'ясуванні місця кібертерористичної протидії в системі кримінологічної безпеки підприємств аерокосмічної галузі України, виділенні та загальній характеристиці елементів системи кримінологічної безпеки підприємств аерокосмічної галузі України.

Методи дослідження: провідними загальнонауковими методами дослідження цієї проблеми є аналіз літератури з проблеми протидії кіберзлочинності; класифікування – з'ясування елементів забезпечення кримінологічної безпеки підприємств аерокосмічної галузі; аналогії; вивчення та узагальнення відомостей.

Результати дослідження: у статті наведено поняття кримінологічної безпеки підприємств аерокосмічної галузі; розкрито систему цієї безпеки та її складники; з'ясовано, що кібертерористична протидія є основною складовою системи кримінологічної безпеки підприємств аерокосмічної галузі України.

Практичне значення: матеріали цієї статті можуть бути корисні для викладачів кримінології вищих навчальних закладів, практичних кримінологів, працівників підприємств аерокосмічної галузі України, які займаються протидією кіберзлочинності.

Ключові слова: система кримінологічної безпеки, протидія кіберзлочинності, аерокосмічна галузь, кібератака, віктимологічна профілактика.

[11] Шелухин Н.Л. О множественности предмета криминологии // Актуальні проблеми науки та освіти: збірник матеріалів XXII підсумкової науково-практичної конференції викладачів МДУ. Маріуполь: МДУ, 2021, С. 68-70.

[12] Shelukhin N.L, Shelukhin AN, On the feasibility of introducing the specialty of criminology and crime prevention at law schools Russian journal of criminology 2019, 13 (5), 707-717

[13] Е. g., Бабаев М.М. Передел собственности и криминологическая безопасность // Современные разновидности российской и мировой преступности: состояние, тенденции, возможности и перспективы противодействия : сб. науч. тр. Саратов : Сателлит, 2005. С. 172–180.; Клейменов М.П., Артемов А.В. Предвидение криминологической безопасности // Вестник Омского университета. Сер. Право. 2004. № 1. С. 113–115.

[14] Криминология : учеб. / под ред. Г.А. Аванесова. М. Юнити-Дана, 2012. 575 с.

Nikolay Shelukhin, Ivan Kharaberiush, Olga Gromova

DER STELLENWERT VON CYBER-TERRORISMUS-GEGENMASSNAHMEN IM SYSTEM DER KRIMINOLOGISCHEN SICHERHEIT VON UNTERNEHMEN IN DER LUFT- UND RAUMFAHRTINDUSTRIE DER UKRAINE

Die Aktualität der Forschung: Die Relevanz des untersuchten Problems ergibt sich aus der Notwendigkeit, Cyber-Terrorismus-Gegenmaßnahmen im Rahmen der Theorien und Institutionen der kriminologischen Wissenschaft auf Unternehmen der Luft- und Raumfahrtindustrie in der Ukraine zu prüfen.

Das Ziel der Forschung: Der Zweck des Artikels ist es, den Stellenwert von Cyber-Terrorismus-Gegenmaßnahmen im System der kriminologischen Sicherheit von Unternehmen der Luft- und Raumfahrtindustrie der Ukraine zu klären, die Elemente des Systems der kriminologischen Sicherheit von Unternehmen der Luft- und Raumfahrtindustrie in der Ukraine hervorzuheben und zu bezeichnen.

Forschungsmethoden: Die führenden allgemeinen wissenschaftlichen Forschungsmethoden zu diesem Problem sind die Analyse der Literatur zum Problem der Bekämpfung der Cyberkriminalität; Klassifizierung – Verständnis der Elemente zur Gewährleistung der kriminologischen Sicherheit von Unternehmen in der Luft- und Raumfahrtindustrie; Analogien; Erforschung und Verallgemeinerung von Informationen.

Forschungsergebnisse: Der Artikel gibt das Konzept der kriminologischen Sicherheit von Luft- und Raumfahrtunternehmen wieder; das System dieser Sicherheit und ihre Komponenten werden offengelegt; es ist geklärt, dass die Bekämpfung des Cyber-Terrorismus die Hauptkomponente des Systems der kriminologischen Sicherheit von Unternehmen der Luft- und Raumfahrtindustrie in der Ukraine ist.

Praktische Relevanz: Die Materialien dieses Artikels können für Kriminologielehrer an Hochschulen, praktische Kriminologen, Mitarbeiter von Unternehmen der Luft- und

protecting the stability of the aerospace industry from various criminological threats.

The elements of this system include:

first, the subjects of criminological security are enterprises of the aerospace industry;

second, measures of a technical, political, ideological, economic, socio-psychological, legal and other nature aimed at creating conditions that exclude or impede the negative impact of criminological threats on protected objects;

third, scientific, financial, material, technical and other support for the implementation of these measures;

fourth, applied scientific and technical developments;

fifth, combating corruption in all its forms.

The task of the system of criminological security of enterprises in the aerospace industry of Ukraine is to ensure sustainable, rhythmic functioning of the above-mentioned enterprises, as well as to maintain a continuous, high level of their protection from criminological threats.

The subjects involved in ensuring the criminological security of enterprises in the aerospace industry include: directly the enterprises themselves and the associations of these enterprises represented by security services; power structures of the state, ensuring their security, represented by the Security Service of Ukraine, the National Police, the Foreign Intelligence Service, the Main Intelligence Directorate of the Ministry of Defense of Ukraine; government; other organizations that have the rights and responsibilities, as well as the means and capabilities to ensure the criminological security of enterprises in the aerospace industry, its individual elements.

The system for ensuring the criminological security of enterprises in the aerospace industry of Ukraine implies three main types of activities carried out by these entities:

- impact on criminological threats;
- protection of relevant objects from criminological threats;
- victimological prevention aimed at ensuring the criminological security of a potential victim. The objects of this line of activity are often persons holding managerial positions at enterprises of the aerospace industry, as well as employees of these enterprises who have information with a limited access regime.

Impact on criminological threats involves active actions of subjects aimed at direct influence on this or that criminological danger that threatens aerospace enterprises. The impact on the criminological threat is realized through its direct elimination, neutralization of its negative impact on the protected objects, as well as the impact on the causes and conditions that contribute to strengthening the positions of this threat. The active impact on criminological threats will be observed, for example, during the implementation of a clear social and legal policy of the state aimed at stabilizing the current legislation and its anti-corruption orientation; concentration of the most important scientific and technical developments at enterprises and institutions of the state form of ownership; development of clear regulation of production and other processes, etc.

In turn, the protection of aerospace enterprises from criminological threats implies a more passive model of behavior and implies the direct protection of protected objects from threats of a criminal and criminogenic nature, as well as protection from those negative consequences that may occur as a result of the impact of these threats. In addition, the criminological protection of aerospace enterprises includes activities to minimize and eliminate the already occurring negative consequences for the objects of protection.

The type of activity to protect aerospace enterprises from criminological threats will be, for example, the filing of income declarations by all senior employees of the aerospace industry, establishing a special procedure for their travel abroad, and avoiding conflicts of interest among industry workers.

c) Cyber-terrorism countermeasures as the main component of the system of criminological security of enterprises in the aerospace industry of Ukraine.

Cyber-terrorism countermeasures can be most comprehensively and fully described from the point of view of criminology, since it is criminology that studies all areas of combating crime: criminal law, economic, psychological, social etc.[15].

Analyzing cyber-terrorism measurements as a component of the system of criminological security of the aerospace enterprises, it is necessary to understand the direction of these measurements. The applied focus of cyber-terrorism countermeasures is in the creation of scientific and technical products that prevent interference in the functioning systems of the aerospace industry of Ukraine and aimed at countering cyber attacks[16*].

Practical activities to counter cyberattacks are proposed to be divided into 2 groups: organizational and technical.

Organizational activities to counter cyberattacks include daily activities carried out by the administration of the enterprise, which are of a preventive nature. These are activities for:

- selection and verification of personnel;
- compliance with internal regulations;
- compliance with protocols (flow charts) for performing certain types of tasks (work, operations);
- training of analysts in ensuring cybersecurity;
- interaction with cyber units of law enforcement agencies and Internet providers[17];
- competent functioning of enterprise security services.

Technical activities to counter cyber attacks include activities to directly respond to them. This type of activity involves specialists in mathematics, programming, analysis and other areas in the field of IT technologies. These are activities for:

- analysis of existing software in order to find vulnerabilities;
- development of new software;
- improvement of existing software;
- immediate response on cyberattacks.

Almost all organizational activities to counter cyberattacks are governed by the law. Since the enterprises of the aerospace industry, which are an element of the criminological security system, are at the same time subjects of economic activity, their activities are regulated by the Economic Code of Ukraine. Thus, in accordance with Article 15 Technical Regulation in the Field of Man-

[15] Е. g., Босхолов С.С., Сидорова Е.З. Понятие системы обеспечения криминологической безопасности образования / Сергей Семенович Босхолов, Екатерина Закариевна Сидорова // Вестник Восточно-сибирского института МВД России. 2020. №3 (94). С.66-73; Ищук Я. Г., Пинкевич Т. В., Смольянинов Е. С. Цифровая криминология. Учебное пособие. М.: Академия Управления МВД России, 2021. 244 с.; Середа В.В. Тероризм: кримінологічна детермінація і кримінально-правова протидія: монографія / В. В. Середа, І. Р. Серкевич; за заг. ред. В. С. Канціра. Львів: ЛьвДУВС, 2016. 188 с.

[16] A cyberattack is an attempt on the information security of a computer system. A cyberattack in the broadest sense of the word (original meaning) is a brainstorming session aimed at finding a way to solve complex problems. One or several highly qualified specialists (hackers) can take part in the attack. As a result of brainstorming, unconventional methods of solving the problem can be invented, or corrections can be made to existing methods.

[17] Fighting against cybercrime: problems and prospects in Ukraine and the world / Andrii Borko, Vadym Nehodchenko, Olena Volobuieva, Ivan Kharaberiush, Yevheniia Lohvynenko // Journal of Legal, Ethical and Regulatory Issues. 2019. Vol. 22, Special Issue 2

Raumfahrtindustrie der Ukraine, die an der Bekämpfung der Cyberkriminalität beteiligt sind, nützlich sein.

Schlüsselwörter: System der kriminologischen Sicherheit, Bekämpfung der Cyberkriminalität, Luft- und Raumfahrtindustrie, Cyberattacke, viktimologische Prävention.

Nikolay Shelukhin, Ivan Kharaberiush, Olga Gromova

LIEU DES CONTRE-MESURES CONTRE CYBERTERRORISME DANS LE SYSTÈME DE SÉCURITÉ CRIMINOLOGIQUE DES ENTREPRISES DE L'INDUSTRIE AÉROSPATIALE DE L'UKRAINE

Actualité de recherche : l'actualité du problème à l'étude est due à la nécessité d'envisager de contrer les cyberattaques contre les entreprises de l'industrie aérospatiale de l'Ukraine dans le cadre des théories et des institutions de la science criminologique.

Objectif de recherche : l'objectif de l'article est de clarifier la place des contre-mesures contre le cyberterrorisme dans le système de sécurité criminologique des entreprises de l'industrie aérospatiale de l'Ukraine, en mettant en évidence et les caractéristiques générales des éléments du système de sécurité criminologique des entreprises dans l'industrie aérospatiale de l'Ukraine.

Méthodes de recherche: principales méthodes générales de recherche scientifique sur cette problématique sont l'analyse de la littérature sur la problématique de la lutte contre la cybercriminalité ; classification : comprendre les éléments permettant d'assurer la sécurité criminologique des entreprises de l'industrie aérospatiale ; analogies ; étude et généralisation de l'information.

Résultats de recherche: l'article donne le concept de sécurité criminologique des entreprises aérospatiales; le système de cette sécurité et ses composants sont divulgués ; il est clair que la lutte contre le cyberterrorisme est la composante principale du système de sécurité criminologique des entreprises de l'industrie aérospatiale en Ukraine.

Pertinence pratique: le contenu de cet article peut être utile aux enseignants de criminologie des

établissements d'enseignement supérieur, aux criminologues praticiens, aux employés des entreprises de l'industrie aérospatiale de l'Ukraine impliquées dans la lutte contre la cybercriminalité.

Mots-clés: système de sécurité criminologique, lutte contre la cybercriminalité, industrie aérospatiale, cyberattaque, prévention victimologique.

Nikolay Shelukhin, Ivan Kharaberiush, Olga Gromova

THE PLACE OF CYBER-TERRORISM COUNTERMEASURES IN THE SYSTEM OF CRIMINOLOGICAL SECURITY OF ENTERPRISES OF THE AEROSPACE INDUSTRY OF UKRAINE

Research Relevance: the relevance of the problem is determined by the need to consider countering cyberattacks on enterprises of the aerospace industry of Ukraine within the framework of theories and institutions of criminological science.

Research Purpose is to clarify the place of cyber-terrorism countermeasures in the system of criminological security of enterprises of the aerospace industry of Ukraine and highlight general characteristics of the system of criminological security of enterprises in the aerospace industry of Ukraine.

Research Methods: the leading general scientific research methods of this research are the analysis of the literature on countering cybercrime; classification – explanation of elements of ensuring criminological security of enterprises of the aerospace industry; analogies; the study and generalization of information.

Research Results: the concept of criminological security of enterprises of the aerospace industry is given, the system of this security and its components are disclosed in the article; it is emphasized that the cyber-terrorism countermeasures are the main component of the system of criminological security of enterprises of the aerospace industry of Ukraine.

Practical Significance: materials of this article may be useful for teachers of criminology of higher

agement of the Economic Code of Ukraine, technical norms (technical regulations, standards, codes of practice and technical conditions) are legal norms or legal norms [18]. It follows that the products obtained as a result of technical activities to counter cyberattacks (development of new software and improvement of the existing one) are legal and governed by the rules of law.

Conclusions

The system for ensuring criminological security of aerospace enterprises consists of: subjects of criminological security; measures aimed at creating conditions that exclude or impede the negative impact of criminological threats on protected objects; all types of ensuring the implementation of these measures; applied scientific and technical developments; combating corruption in all its forms.

Organizational and technical activities to counter cyberattacks by aerospace enterprises are governed by the law and are legal activities. The components of the system of countering cyber attacks are described by the theories and institutions of criminology.

Cyber-terrorism is an element of the system of criminological security of enterprises in the aerospace industry in Ukraine. Cyber-terrorism countermeasures are organizational and technical in nature.

During the study, new questions and problems arose that need to be addressed. It is necessary to continue research on the development of regulatory legal acts in the field of countering cyberattacks on enterprises of the aerospace industry in Ukraine, studying the phenomenon of countering cyberattacks on enterprises in the aerospace industry from the point of view of law; on the development of the criminological theory for combating cybercrime at critical infrastructure facilities.

Recommendations

The materials of this article can be useful for teachers of criminology of higher educational institutions, practical criminologists, employees of enterprises of the aerospace industry of Ukraine involved in combating cybercrime.

References

Fighting against cybercrime: problems and prospects in Ukraine and the world / Andrii Borko, Vadym Nehodchenko, Olena Volobuieva, Ivan Kharaberiush, Yevheniia Lohvynenko // Journal of Legal, Ethical and Regulatory Issues. 2019. Vol. 22, Special Issue 2 [in English].

Financial and legal regulation of electronic money circulation in developed countries / Semen Stetsenko, Olena Yu. Syniavska, Mykola L. Shelukhin, Serhii Lukash, Yevhen Barash // Journal of Legal, Ethical and Regulatory Issues. 2019. Vol. 22, Special Issue 2 [in English].

Collin, B., 1997. The Future of Cyberterrorism. Crime & Justice International Journal. Vol. 13(2). P. 15-18 [in English].

Plotov, V. I. & Mikhailov D. M. & Pedanov, V. A., 2020. Ugrozy terrorizma v usloviyakh tsifrovoi transformatsii mira i puti zashchity ot nikh [Terrorism Threats in the Context of the Digital Transformation of the World and Ways to Defend Against Them]. Gumanitarnye nauki. Vestnik Finansovogo universiteta. 10(1):14-20. [in Ukrainian].

World Economic Forum. URL: https://www.weforum.org/ [in English].

Puti k kiberustoychivoy aviatsionnoy otrasli [Pathways to a Cyber Resilient Aviation Industry]. Published: April 14, 2021. URL: http://www3.weforum.org/docs/WEF_Pathways_Cyber_Resilient_Aviation_2021.pdf [in Russian].

Plan deistvii po obespecheniyu kiberbezopasnosti Mezhdunarodnoi organizatsii grazhdanskoi aviatsii [International Civil Aviation Organization Cybersecurity

[18] Господарський кодекс України 16 січня 2003 року № 436-IV // Відомості Верховної Ради України, 2003, № 18, № 19-20, № 21-22, ст.144.

Action Plan]. Opublikovano 5 noyabrya 2020 goda. URL: https://m.favt.gov.ru/public/materials//1/7/e/3/b/17e3bdfb0c48411080846e9b7116f8aa.PDF [in Russian].
Strategiya IKAO v oblasti kiberbezopasnosti [ICAO Cybersecurity Strategy]. Prinyato na assamblei 40 sessii IKAO 25.06.2019 goda. URL: https://www.icao.int/Meetings/a40/Documents/WP/wp_028_ru.pdf [in Russian].
Sovershenstvovanie kontseptsii kiberbezopasnosti v aviatsii [Improving the concept of cybersecurity in aviation]. Reshenie 13 Aeronavigatsionnoi konferentsii. Monreal, Kanada, 9–19 oktyabrya 2018 god. URL: https://www.icao.int/Meetings/anconf13/Documents/WP/wp_042_ru.pdf [in Russian].
Prognosty`chne modelyuvannya komp'yuterny`x virusny`x epidemij [Prognostic modeling of computer viral epidemics]: monografiya / Shevchenko V.L., Nesterenko O. V., Netesin I. Ye., Shevchenko A. V. Ky`yiv: UkrNCz RIT, 2019. 152 s. [in Ukrainian].
Mezhdunarodnaya bezopasnost, strategicheskaya stabilnost i informatsionnye tekhnologii [International Security, Strategic Stability and Information Technology] / otv. red. A. V. Zagorskii, N. P. Romashkina. M.: IMEMO RAN, 2020. 98 s. [in Russian].
Stepanov, O., 2021. Protivodeistvie kiberterrorizmu v tsifrovuyu epokhu [Countering cyber terrorism in the digital age]. M.: Yurait. 103 s. [in Russian].
Begishev, I. R. & Bikeev, I. I., 2020. Prestupleniia v sfere obrashcheniia tsifrovoi informatsii [Crimes in the sphere of circulation of digital information]. Kazan: «Poznanie» KIU. 300 s. [in Russian].
Cyber War: Law and Ethics for Virtual Conflicts / Jens David Ohlin, Kevin Govern, and Claire Finkelstein, Oxford Scholarship Online, 2015. DOI: 10.1093/acprof:oso/9780198717492.001.0001 [in English].
Counter-Terrorism. The Ethical Issues / Edited by Seumas Miller. Open access books. 2021. 224 p. [in English].
Robert, J., 2020. Bunker, Terrorism Futures: Evolving Technology and TTPS Use (Indianapolis, IN: Xlibris/A C/O Futures Pocketbook, 2020). 160 p. [in English].
Gus Martin, 2021. Understanding Terrorism: Challenges, Perspectives, and Issues [7th Edition] (Los Angeles, CA: SAGE). 592 p. [in English].
Douglas Pratt, 2018. Religion and Extremism: Rejecting Diversity (New York, NY: Bloomsbury Academic/An Imprint of Bloomsbury Publishing Plc.). 208 p. [in English].
Jez Littlewood, Lorne L. Dawson, and Sara K. Thompson (Eds.), 2020. Terrorism and Counter-Terrorism in Canada (Toronto, Canada: University of Toronto Press). 352 p. [in English].
Gorsheneva, I. A. & Goltseva, O. Yu., 2019. Osobennosti protivodeistviya prestupleniyam kiberterroristicheskoi napravlennosti (Zarubezhnyi opyt) [Features of countering cyber-terrorist crimes (Foreign experience)] // Kriminologicheskii zhurnal. №3. S.10-16 [in Russian].
Nazarov, V. L. & Osipchukova, E. V., 2015. Mezhdunarodnyi opyt profilaktiki ekstremizma [International experience in the prevention of extremism]: ucheb. posobie. Ekaterinburg: Izd-vo Ural. un-ta. 248 s. [in Russian].
Ekstremizm i terrorizm v kiberprostranstve: ugrozy miru i bezopasnosti chelovechestva [Extremism and terrorism in cyberspace: threats to the peace and security of mankind]: sbornik statei po itogam III Vserossiiskoi studencheskoi nauchnoprakticheskoi ochno-zaochnoi videokonferentsii / pod red. V.A. Mazurova, M.A. Starodubtsevoi. Barnaul: Izd-vo Alt. un-ta, 2020. 203 s. [in Russian].
Shelukhin, N. L., 2021. O mnozhestvennosti predmeta kriminologii [On the plurality of the subject of criminology] // Aktual`ni problemy` nauky` ta osvy`ty`: zbirny`k materialiv XXII pidsumkovoyi naukovo-prakty`chnoyi konferenciyi vy`kladachiv MDU Mariupol`: MDU. S. 68-70 [in Ukrainian].
Shelukhin, N. L & Shelukhin, A. N., 2019. On the feasibility of introducing the specialty of criminology and crime prevention at law schools Russian journal of criminology. 13 (5), 707-717 [in English].
Babaev, M. M., 2005. Peredel sobstvennosti i kriminologicheskaya bezopasnost [Property redistribution and criminological security] // Sovremennye raznovidnosti rossiiskoi i mirovoi prestupnosti: sostoyanie, tendentsii, vozmozhnosti i perspektivy protivodeistviya: sb. nauch. tr. Saratov: Satellit. S. 172–180 [in Russian].
Kleimenov, M. P. & Artemov, A. V., 2004. Predvidenie kriminologicheskoi bezopasnosti [Foresight of Criminological Safety] // Vestnik Omskogo universiteta. Ser. Pravo. № 1. S. 113–115 [in Russian].

educational institutions, practical criminologists, employees of the aerospace industry of Ukraine, involved in countering cybercrime.

Keywords: system of criminological security, countering cybercrime, aerospace industry, cyberattack, victimological prevention.

Kriminologiya [Criminology]: ucheb. / pod red. G.A. Avanesova. M. : Yuniti-Dana, 2012. 575 s. [in Russian].

Boskholov, S. S. & Sidorova, Ye. Z., 2020. Ponyatiye sistemy obespecheniya kriminologicheskoy bezopasnosti obrazovaniya / Sergey Semenovich Boskholov, Yekaterina Zakariyevna Sidorova // Vestnik Vostochno-sibirskogo instituta MVD Rossii. 2020. № 3 (94). S. 66-73.

Ishchuk, Ya. G. & Pinkevich, T. V. & Smolyaninov, E. S., 2021. Tsifrovaya kriminologiya [Digital criminology]: uchebnoe posobie. Moskva: Akademiya upravleniya MVD Rossii. 244 s. [in Russian].

Terory`zm: kry`minologichna determinaciya i kry`minal`no-pravova proty`diya [Terrorism: criminological determination and criminal law counteraction]: monografiya / V. V. Sereda, I. R.Serkevy`ch; za zag. red. V. S. Kancira. L`viv: L`vDUVS, 2016. 188 s. [in Ukrainian].

Gospodars`ky`j kodeks Ukrayiny` [Economic Code of Ukraine] 16 sichnya 2003 roku № 436-IV // Vidomosti Verxovnoyi Rady` Ukrayiny`, 2003. №№18, 19-20, 21-22. st. 14 [in Ukrainian].

Received by Editorial Board: 16.09.2021

Suggested Citation:

Shelukhin, N., Kharaberiush, I., Gromova, O., (2021). Fire and Technical Aspects Related to Fire of Lithium-Ion Batteries. Archives of Criminology and Forensic Sciences. 2(4). 60-69. DOI: https://doi.org/10.32353/acfs.4.2021.05