Nataliia Filipenko,
Doctor of Law, Professor, Professor of the Law Department of National Aerospace University of National Aerospace University – "Kharkiv Aviation Institute" NAU "KhAI", Kharkiv, Ukraine
e-mail: n.filipenko@khai.edu
ORCID: 0000-0001-9469-3650
Hanna Spitsyna,
Doctor of Law, Professor, First Deputy Director of National Scientific Center «Hon. Prof. M. S. Bokarius Forensic Science Institute», Kharkiv, Ukraine
ORCID: 0000-0001-9131-0642
spitsyna_hanna@ukr.net
Aleksandar Ivanović,
Doctor of Law, Professor,
Director of Forensic Center Montenegro
Danilovgrad, Montenegro

CERTAIN ISSUES OF APPLYING ARTIFICIAL INTELLIGENCE AND INFORMATION COMMUNICATIONS TECHNOLOGIES IN PREVENTING CYBERTERRORIST ATTACKS ON CRITICAL INFRASTRUCTURE FACILITIES

Introduction. "Artificial intelligence" technologies are increasingly affecting various areas of social life, determining not only the level of capabilities but also how well social values are protected [1, p. 1086].

Every week, networks seem to grow in size and complexity. New SaaS services come online, while innovative communication tools make remote working easier. Data storage methods shift, with new assets to secure. And new malware threats constantly emerge. In an ever-changing digital world, network security has never been more crucial. Network security is not a fixed constant. Methods to protect networks change all the time [2].

With the constant expansion and emergence of new digital capabilities, most countries worldwide have bolstered their cybersecurity measures. Consequently, new real and potential threats have emerged, broadening the scope of cyberattacks [3, p. 98] that target critical and socially significant infrastructure. This necessitates ensuring the resilience of both governmental and private corporate systems and networks.

Literature Review. Particular issues on application of artificial intelligence and information and communications technologies in preventing cyber terrorist attacks on critical infrastructure facilities have been addressed by scholars such as V. V. Vertuzaiev, V. V. Holina, M. V. Karchevskyi, V. K. Kolpakov, S. Yu. Lukashevych, M. I. Panov, H. O. Spitsyna, L. K. Tereshchenko, T. I. Tarakhonych, B. S. Ukraintsev, N. Ye. Filipenko, V. S. Frolov, V. M. Shevchuk,

V. Yu. Shepitko, A. V. Chernykh, S. V. Yasechko, and others. However, many theoretical and applied issues remain debatable and require further clarification and development, particularly in conditions of the Russian Federation's armed aggression against Ukraine.

Results and discussion. The most dangerous and devastating consequences are attributed to terrorist acts involving the use of weapons, ammunition, or explosives, as they pose a real threat to human life and health and cause destruction to industrial, economic, or defense facilities. Complexity of investigating these crimes is explained by the following factors: rapid advancements in the field of armaments; flaws in controlling the movement of weapons and ammunition; corruption and deficiencies in organizational and economic practices within the Armed Forces of Ukraine; large gaps in national-patriotic education of population; a high level of stress and psychological burden on society; emergence of panic moods fueled by negative military, economic, and social factors; activities of numerous informal military-type associations; growing societal tendencies towards the use of force in conflict resolution, proliferation of brutality and violence; low coordination of activities among law enforcement agencies in counter-terrorism operations; the presence of a vast database sourced from the open Internet concerning the manufacturing and utilization of weapons and explosive devices; the availability of readily accessible tools with so-called "dual" purpose, which can be used as components for homemade weapons or explosive devices; the widespread presence of websites on the Internet promoting extremist ideologies, etc. [4, p. 189].

Critical infrastructure is, and will continue to be, particularly vulnerable to terrorist attacks, and targeting it will have the most devastating effect. The United Nations policy papers emphasize that «there remains a pressing need to redouble efforts and reaffirm commitments to the full promotion and protection of human rights and fundamental freedoms across all efforts to counter-terrorism and prevent violent extremism conducive to terrorism» [5].

Critical infrastructure facilities are of interest for several reasons. Firstly, they can be attractive targets due to their strategic value to society, especially in highly industrialized countries of the Western hemisphere. Disrupting the functioning of these facilities, ideally with the potential to generate cascading effect, allows terrorists to maximize damage with just one strike and instill fear to a degree that would be difficult to achieve by targeting "ordinary" (less crucial) facilities. Secondly, they can serve to highlight the powerlessness of state institutions. For example, terrorist organizations may choose to attack energy infrastructure facilities, pipelines, etc., in order to disrupt the provision of basic services and reveal the fragility of government agencies and associated policies, etc. [6].

The Law of Ukraine *On the Basic Principles of Cybersecurity in Ukraine* No. 2163-VIII [7] dated October 5, 2017 defines the protection of vital interests of a person and citizen, society and the state in the use of cyberspace as sustainable development of the information society and digital communications environment, timely identification, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace.

Widespread digital communication leads to the emergence of new methods for conducting cyberterrorist attacks on critical infrastructure facilities, mechanisms for creating and operating organized terrorist groups, and increasing the complexity of the forms and methods of their criminal activities.

Cyber threats vary, but may include, for example: manipulation of systems or data (i.e., malware exploiting vulnerabilities in computer software and hardware components necessary for the operation of critical infrastructure or life support); disabling critical systems, such as denial-of-service attacks; and restricting access to critical systems or information (i.e., through ransomware attacks, deploying malicious software via removable media and external devices, etc.).

The most dangerous of such attacks are considered Advanced Persistent Threats (APTs). APT attacks are targeted cyberattacks on the computer networks of competitors (organizations, states), utilizing latent (not outwardly manifested) vulnerabilities in conjunction with covert reconnaissance or subversive actions. Their primary goal is to obtain, disrupt the integrity of, or block information vital to another state.

Data regarding the series of cyber attacks that occurred in Ukraine, primarily targeting our state's critical infrastructure, were disclosed at the Virus Bulletin conference and within the framework of the Cisco forum *Cybersecurity Technologies* (December 8, 2016). Among the various known methods of initiating cybersecurity incidents, the infection of users with malicious software is unequivocally recognized as the most prevalent (70.2%). In 2016, attackers predominantly utilized zero-day attacks for this purpose. Following these are spam, phishing, and various types of internet fraud (52.5%), DOS attacks (37.4%), spyware attacks (20%), ransomware (18.5%), targeted hacker attacks (15.1%), and botnets (12.5%).

Conclusions. In light of the above, we believe it is necessary to suggest the following methods to counter cyberterrorist attacks on critical infrastructure facilities, namely:

1. Develop risk profiles for specific sectors and critical infrastructure facilities. These profiles are crucial for assessing existing mitigation practices, outcomes, and vulnerabilities. Depending on the sector under consideration, risk assessments may be conducted for specific facilities. For example, Australia's Critical Infrastructure Resilience Strategy breaks down the transportation sector into the following subsectors: aviation, land passenger transport (including bridges and tunnels), land transport, and maritime transport (shipping and ports). In alignment with the same strategy, the energy sector consists of electricity supply systems, offshore oil and gas fields, and onshore oil, gas, and coal supplies.

2. Create schemes for organizing cybersecurity at critical infrastructure facilities. Such a scheme contains key elements of cyber attacks on critical infrastructure facilities and offers options for their protection against possible cybercriminal actions. In this case, following the scheme, each cyber attack can be presented as a specific algorithm of actions, the use of which will significantly streamline the process of organizing cybersecurity and increase the efficiency of decisions made.

3. Extensive cooperation among governmental, commercial, and public structures in developing conceptual frameworks and recommendations for countering cyberterrorist attacks on critical infrastructure facilities.

References:

1. Філіпенко Н.Є., Лукашевич С.Ю. (2023) Інформаційні методики дослідження кримінальних правопорушень, вчинених з використанням технологій штучного інтелекту. Наукові перспективи (Серія «Державне управління», Серія «Право», Серія «Економіка», Серія «Медицина», Серія «Педагогіка», Серія «Психологія») Випуск № 11(41)2023. Київ. 2023. № 1(7). С. 1084-1096.
2. Network security basics. URL: https://nordlayer.com/learn/network-security/basics/
3. Leblanc S.P., Partington A., Chapman I.M., Bernier M. An overview of cyber attack and computer network operations simulation. SpringSim (MMS), 2011, pp. 92-100.
4. Спіцина Г. О., Філіпенко Н. Є. Терористична діяльність: кримінально-правова політика протидії // Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку : зб. тез доп. міжнар. наук.-практ. конф. до 25-річчя ХНУВС (18 квіт. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Кримінол. асоц. України. Харків : ХНУВС, 2019. С. 188-191.
5. UN Global Counter-Terrorism Strategy Special Rapporteur on counter-terrorism and human rights. URL: https://www.ohchr.org/en/special-procedures/sr-terrorism/un-global-counter-terrorism-strategy#:~:text=The%20UN%20Global%20Counter-Terrorism%20Strategy%20(A%2FRES%2F,States%27%20counter-terrorism%20priorities.
6. Акерман 2007, Оцінка мотивації терористів для нападу на критично важливі інфраструктури, Центр досліджень з нерозповсюдження, Монтерейський інститут міжнародних досліджень. URL: https://e-reports-ext.llnl.gov/pdf/341566.pdf
7. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text