DOI: https://doi.org/10.32353/acfs.10.2024.01
UDC 343.98 (477)

Oleksii Lytvynov

Nataliia Filipenko

Oleksii Lytvynov
Doctor of Law, Professor, Rector of National Aerospace University of National Aerospace University — "Kharkiv Aviation Institute" NAU "KhAI", Ukraine
ORCID: https://orcid.org/0000-0003-2952-8258
e-mail: khai@khai.edu

Nataliia Filipenko
Doctor of Law, Professor, Professor of the Law Department of National Aerospace University of National Aerospace University — "Kharkiv Aviation Institute" NAU "KhAI", Ukraine
ORCID: https://orcid.org/0000-0001-9469-3650
e-mail: n.filipenko@khai.edu

Hanna Spitsyna
Doctor of Law, Professor, First Deputy Director of National Scientific Center «Hon. Prof. M. S. Bokarius Forensic Science Institute», Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0001-9131-0642
e-mail: spitsyna_hanna@ukr.net

Aleksandar Ivanović
Doctor of Science, regular university professor, adviser, Police Administration of Montenegro,
e-mail: ialeksandar@t-com-me

Cyber Polygon — Practice of Protecting Critical Infrastructure Objects and Companies of Aviation Industry from Cyber Terrorist Attacks — Experience of Ukraine and the World (Review article)

The article discusses development and implementation of a set of measures to ensure information and cyber terrorist security at critical infrastructure facilities and enterprises of the aerospace industry with the development of measures to counter hybrid criminal influences. The authors propose the creation of cyber polygons that provide an opportunity to study complex cyber terrorist attacks and train cybersecurity specialists.

The foreign experience of modeling cyber terrorist attacks during large-scale cyber exercises is analyzed, which can be used in the development of cyberattack scenarios in domestic cyber polygon technologies to train specialists in the conditions of rapid development of technologies and growing cybersecurity risks. Based on the generalization of experience, tactical and organizational measures to prevent cyber-terrorist attacks on critical infrastructure facilities and aerospace enterprises are proposed.

Keywords: critical infrastructure facilities, aerospace industry enterprises, cyber polygon, cyber terrorist threat, cybersecurity.

Introduction. Threats to critical infrastructure, such as cyberattacks, terrorist acts, sabotage and military aggression are becoming increasingly relevant in modern globalized world. One of the main reasons for this is that critical infrastructure includes systems that support the livelihoods of the state and its citizens; these are energy, aerospace, water supply, transport, financial systems and health care. Damage to any of these systems can lead to catastrophic consequences not only for a particular region, but at the international level.

Terrorist attacks on critical infrastructure facilities are aimed at undermining not only material resources, but also the morale of the population, creating a sense of danger. In this context, terrorist acts can cause explo-

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 authors 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.

sions or physical attacks on high-risk objects: nuclear power plants, aerospace enterprises, hydraulic structures or transport systems[1].

Military actions pose a great danger to critical infrastructure facilities. The military aggression of the Russian Federation against Ukraine is constantly accompanied by deliberate attacks on infrastructure to undermine the economic capacity of our country and destabilize its operation[2]. According to data, military operations on the territory of Ukraine by the armed forces of the aggressor country do not avoid nuclear energy facilities (Zaporizhzhya and South Ukrainian NPPs), which poses a serious potential threat to the whole world. Missile and artillery shelling of Ukraine's energy sector facilities has a negative impact on the security of critical infrastructure. In particular, significant damage was caused by shelling of the energy system: Dnipro, Kremenchuk, Kyiv, Kakhovka hydropower plants, Kyiv, Trypillia, Kharkiv, Starobesheve, Sloviansk, Myronivka, Luhansk, Kurakhivka, Zuiv, Zmiiv, Zaporizhzhia, and Vuhlehirsk thermal power plant. Infrastructure facilities that support the vital functions of the population, power grids, electricity generation and transmission facilities, water utilities, heat and gas networks, telephone lines, etc. are constantly under fire throughout Ukraine. This is particularly acute in Zaporizhzhia, Kherson, Mykolaiv regions, occupied, de-occupied and military affected areas.

Hanna Spitsyna

Aleksandar Ivanović

Significant damage (partial or complete destruction) due to the conduct of hostilities has been caused to port facilities, transport routes, bridges, crossings, industrial facilities, oil pipelines and storage facilities; gas pipelines and other critical infrastructure facilities throughout the territory of our State[3].

The war has a significant impact on the aerospace industry, creating a number of dangers. Military actions can lead to an increase in aviation accidents due to possible attacks on airports, aircraft and other infrastructure, which has a multiplier effect on the risk of significant human casualties and economic losses. Disruptions in the operation of aviation and space infrastructure due to destruction or damage to facilities can lead to disruptions in the supply of goods and services, as well as problems with communications and navigation. In addition, there are very high risks of reducing investment in the aerospace industry due to the uncertainty and dangers associated with the war. This can lead to a slowdown in the development of the industry and the loss of jobs.

Among the greatest threats to critical infrastructure facilities, it is worth highlighting cyber-terrorist attacks that can disrupt the operation of information systems responsible for managing infrastructure facilities, which can threaten the safety of millions of people. This makes them particularly vulnerable to outside interference.

Analysis of publications where this problem solution is initiated. In general, the issue of protecting critical infrastructure facilities from cyber-terrorist attacks is devoted to the work of many scientists, in particular: O. M. Bandurka, V. V. Bondar, V. S. Batyrhareieva, Yu. V. Kuzmenko, O. M. Lytvynov, Yu. V. Orlov, H. O. Spitsyna, N. Ye. Filipenko, V. Yu. Shepitko et al4. How-

[1] 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.

[2] Кузьменко Ю. В., Коропатов О. М., Думанський Р. В. Адміністративно-правове забезпечення захисту об'єктів критичної інфраструктури України під час воєнного стану. *Юридичний Бюлетень.* Випуск 27. 2022. DOI https://doi.org/10.32850/LB2414-4207.2022.27.08 с. 63

[3] Там само, с. 64

[4] Див. докладніше: Батиргареєва В. С., Бабенко А. М. Аналіз сучасної криміногенної ситуації в Україні як інформаційна модель для розробки стратегії зменшення можливостей вчинення злочинів. *Архів кримінології та судових наук* : наук. журнал / Ред. кол.: О. М. Клюєв, В. С. Батиргареєва, Г. О. Спіцина та ін. Харків : ХНДІСЕ, 2020. No. 1. С 39–53; Mykola Nechyporuk, Volodymyr Pavlikov, Nataliia Filipenko, Hanna Spitsyna, Ihor Shynkarenko Cyberterrorism Attacks on Critical Infrastructure and Aviation: Criminal and Legal Policy of Countering. Integrated Computer Technologies in Mechanical Engineering – 2020. Synergetic Engineering P. 206–220. ISBN 978-3-030-66716-0 ISBN 978-3-030-66717-7 (eBook). URL: https://doi.org/10.1007/978-3-030-66717-7; Філіпенко Н. (2022) Протидія кібератакам на об'єкти

O. Lytvynov, N. Filipenko, H. Spitsyna, A. Ivanović

CYBER TRAINING GROUND – THE PRACTICE OF PROTECTING CRITICAL INFRASTRUCTURE FACILITIES AND AEROSPACE INDUSTRY ENTERPRISES FROM CYBER TERRORIST ATTACKS – EXPERIENCE OF UKRAINE AND THE WORLD (review article)

The article deals with the issues of development and implementation of a set of measures to ensure information and cyber-terrorist security at critical infrastructure facilities and aerospace enterprises with the development of measures to counteract hybrid criminal influences. The authors propose the creation of cyber training grounds that provide an opportunity to study complex cyber terrorist attacks and train cybersecurity specialists.

The author analyzes the foreign experience of modeling cyber terrorist attacks during large-scale cyber exercises, which can be used to develop cyber attack scenarios in domestic cyber training grounds technologies to train specialists in the context of rapid technological development and growing cybersecurity risks. Based on the generalization of experience, tactical and organizational measures to prevent cyberterrorist attacks on critical infrastructure facilities and aerospace enterprises are proposed.

Keywords: critical infrastructure facilities, aerospace industry enterprises, cyber training ground, cyber terrorist threat, cybersecurity.

ever, most scientists developed one or more aspects of the problem at hand without solving the problem in a comprehensive, integrated way. Particularly undeveloped are the issues of protecting critical infrastructure facilities and enterprises of the aerospace industry during the war, as well as the use of best practices of foreign states in Ukraine to overcome these threats and minimize risks and damages.

Results and discussion. Cyber-terrorist attacks are one of the greatest threats of our time, since they can paralyze not only individual businesses or organizations, but also entire state institutions. Such attacks can cause serious disruptions in the operation of critical infrastructure facilities, aerospace enterprises, telecommunications systems, which are critical for coordinating the activities of emergency services, medical institutions, police and other organizations responsible for protecting the life and safety of citizens. Malfunctioning of such systems can lead to significant delays in responding to accidents, catastrophes or other emergencies, which, in turn, poses a real threat to the life and health of many people.

During the full-scale war, the number of cyberattacks in Ukraine has increased several times compared to previous years. Since February 24, 2022, more than 4,500 cyberattacks have been recorded. In 2020, there were only 800 of them and in 2021, about 2,000[5].

This highlights the need for continuous improvement of cybersecurity systems and proper training of information security professionals to ensure the resilience of national systems.

In a number of public and private organizations, in the conditions of isolation and increase of employees working remotely, there was an experience of active transfer of part of their activities to the Internet6. In this regard, new real and potential threats have emerged, the range of cyberattacks on critical and socially significant infrastructure has expanded, which requires ensuring the sustainability of the functioning of public and private corporate systems and networks. Ensuring their sustainability is facilitated by the simulation of cybercrime scenarios — a set of interrelated and interdependent actions and operations of their participants in cyberspace — the creation of state-of-the-art cyber polygons.

As scientists note, a cyber polygon is a collection of software and hardware tools united by a single distributed local network with access to the Internet, which is intended for working out applied issues of development, design and testing of software and technical systems (complexes) providing information (informational and psychological) and cyber security in the course of implementing the functions of monitoring, protection and active influence, conducting multilateral exercises, ensuring the generalization of experience,

критичної інфраструктури та життєзабезпечення під час військової агресії проти України. Український дослідницький простір в умовах війни: адаптація й перезавантаження технічних і юридичних наук: збірник матеріалів доповідей учасників міжнародної науково-практичної конференції. (Харків-Рига, 31 травня 2022 р.). Харків, 2022. С. 213-217.; Кузьменко Ю.В., Бондар В.В. Захист об'єктів критичної інфраструктури: адміністративно-правове забезпечення. *Юридичний бюлетень*. 2021. Вип. 21. С. 67–72. та ін.

[5] Національний центр резервування державних інформаційних ресурсів (НЦ). URL: https://uss.gov.ua/service/natsionalnyj-tsentr-rezervuvannya-derzhavnyh-informatsijnyh-resursiv-nts/#:~:text=За%20час%20повномасштабної%20війни%20кількість,а%20в%202021%20–%20близько%202000.

[6] Lallie H. S., Shepherd L. A., Nurse J. R. C., Erola A., Epiphaniou G., Maple C., Bellekens X. (2021). Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers and Security, 105, [102248]. URL: http://doi.org/10.1016/j.cose.2021.102248

the development of forms, methods and methods of forecasting, prevention, detection and countermeasures against crisis situations in cyberspace, the implementation of practical training, retraining and upgrading of military personnel (civilian) specialists (according to national and NATO standards), as well as for conducting fundamental and applied scientific research in the field of information and cyber security and cyber defense of the state[7].

Cyber polygons will become a platform for researching complex cyber-terrorist operations and training qualified cybersecurity specialists. The main purpose of such cyber polygons is to develop and implement methodologies that will provide automated monitoring of cyberspace, analytical data processing, forecasting of possible threats and planning of countermeasures. Both passive and active protection measures play an important role, which will allow to respond more effectively to information threats and protect critical infrastructure. Cyber polygons will also become a tool for simulating real attacks in a virtual environment that will allow you to work out scenarios for responding to threats in a safe environment, while increasing the level of competence of specialists in this field.

In Ukraine, from the end of 2020, such technologies began to be systematically developed and from 2021-2022, they were introduced into the life and activities of law enforcement agencies. In educational institutions, through the use of new technologies, measures are being taken to reduce the gap between the spread of distance learning methods using geographically distributed information systems and the insufficient level of their protection.

For example, Military Institute of Telecommunications and Informatization of the Armed Forces of Ukraine received a cybersecurity training complex, which is designed to detect, respond to, counter and prevent cyber threats. The complex can be used to analyze and investigate cyber incidents, it is designed to improve the quality of the educational process (E.g., figure). The complex includes software and hardware, a situational center, a complex of technical means and includes 80 automated workplaces for cadets and students of the institute studying in Cybersecurity specialization[8].

Globalization leads to the strengthening of interconnection of state and private structures. The private security service is also developing rapidly in Ukraine. Thus, the Unit Range[9] cyber training ground was launched, which was created for the practical training of cyber security specialists in conditions as close as possible to real ones. There are already more than 150 scenarios in the system, and specialists from Ukrainian state and private bodies are trained. Rehearsal of cyber actions is carried out in a closed virtual environment that simulates the real infrastructure that cyber security specialists will have to attack or defend, depending on the profile of the activity. This is usually a cloud solution on virtual machines (we have everything in Amazon Web Services), where scenarios developed by cyber security experts are deployed. Such scenarios simulate hacker attacks as much as possible, or systems that need to be attacked (if you train offense). Unit Range was created directly during the war, and its developers took

[7] Даник, Ю. Г. (2019) Особливості створення кіберполігонів для дослідження комплексних кібердій та підготовки фахівців з кібербезпеки. Confrontation in the cybernetic. *Modern Information Technologies in the Sphere of Security and Defence* № 1(34)/2019. DOI:10.33099/2311-7249/2019-34-1-95-102

[8] ВІТІ отримав кіберполігон. URL: https://mil.in.ua/uk/news/viti-otrymav-kiberpoligon/

[9] Єгор Аушев запустив кіберполігон для тренування спеціалістів — там вже є понад 150 сценаріїв атаки і захисту. URL: https://dou.ua/lenta/news/about-unit-range/

O. Lytvynov, N. Filipenko, H. Spitsyna, A. Ivanović

CYBER-ÜBUNGSGELÄNDE — DIE PRAXIS DES SCHUTZES KRITISCHER INFRASTRUKTUREINRICHTUNGEN UND UNTERNEHMEN DER LUFT- UND RAUMFAHRTINDUSTRIE VOR CYBER-TERRORISTISCHEN ANGRIFFEN — ERFAHRUNGEN DER UKRAINE UND DER WELT (Übersichtsartikel)

Zusammenfassung. Der Artikel befasst sich mit der Entwicklung und Umsetzung eines Maßnahmenpakets zur Gewährleistung der Informations- und Cyber-Terrorsicherheit bei kritischen Infrastruktureinrichtungen und Unternehmen der Luft- und Raumfahrtindustrie sowie mit der Entwicklung von Maßnahmen zur Bekämpfung hybrider krimineller Einflüsse. Die Autoren schlagen die Schaffung von Cyber-Trainingsgeländen vor, die die Möglichkeit bieten, komplexe cyber-terroristische Angriffe zu studieren und Cybersicherheitsspezialistenauszubilden.

Der Autor analysiert die ausländischen Erfahrungen mit der Modellierung von Cyber-Terrorangriffen während groß angelegter Cyber-Übungen, die für die Entwicklung von Cyber-Angriffsszenarien in inländischen Cyber-Trainingsgelände-Technologien für die Ausbildung von Spezialisten im Zusammenhang mit der rasanten technologischen Entwicklung und den wachsenden Cybersicherheitsrisiken genutzt werdenkönnen.Schlüsselwörter: kritische Infrastruktureinrichtungen, Unternehmen der Luft- und Raumfahrtindustrie, Cyber-Trainingsgelände,cyberterroristische Bedrohung, Cybersicherheit.

O. Lytvynov, N. Filipenko, H. Spitsyna, A. Ivanović

CYBER TRAINING GROUND – LA PRATIQUE DE LA PROTECTION DES INFRASTRUCTURES CRITIQUES ET DES ENTREPRISES DE L'INDUSTRIE AÉROSPATIALE CONTRE LES CYBERATTAQUES TERRORISTES – L'EXPÉRIENCE DE L'UKRAINE ET DU MONDE ENTIER (article de synthèse)

Résumé. L'article traite de l'élaboration et de la mise en œuvre d'un ensemble de mesures visant à garantir la sécurité de l'information et la protection contre le cyberterrorisme dans les infrastructures critiques et les entreprises aérospatiales, ainsi que de l'élaboration de mesures visant à contrecarrer les influences criminelles hybrides. Les auteurs proposent la création de terrains d'entraînement cybernétique permettant d'étudier des attaques cyberterroristes complexes et de former des spécialistes de la cybersécurité.

L'auteur analyse l'expérience étrangère en matière de modélisation des attaques cyberterroristes lors d'exercices cybernétiques à grande échelle, qui peut être utilisée pour élaborer des scénarios de cyberattaques dans les technologies des terrains d'entraînement cybernétiques nationaux afin de former des spécialistes dans le contexte du développement technologique rapide et des risques croissants en matière de cybersécurité. Sur la base de la généralisation de l'expérience, des mesures tactiques et organisationnelles sont proposées pour prévenir les attaques cyberterroristes contre les infrastructures critiques et les entreprises aérospatiales.

Mots clés : installations d'infrastructures critiques, entreprises de l'industrie aérospatiale, terrain d'entraînement cybernétique, menace cyberterroriste, cybersécurité.

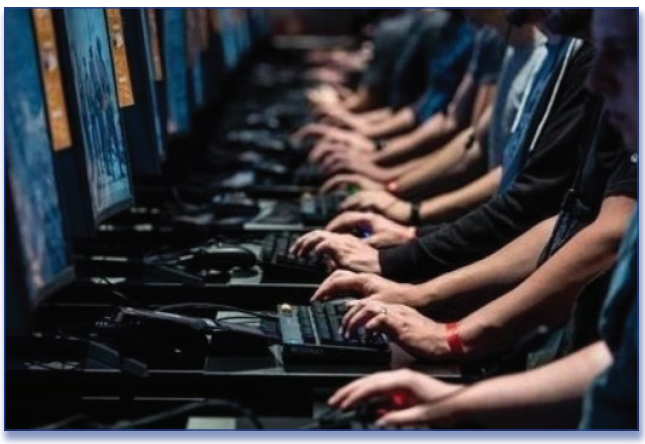
into account the features of modern warfare, where combat operations are often combined with cyberattacks and attempts to destroy the enemy's digital infrastructure. In addition, Unit Range provides a real-time data dashboard that measures the performance and risk profile of all team members, from executives to regular IT staff.

Increased connectivity of information and cyber-physical systems creates additional risks in the field of ensuring information security, therefore system risk management requires cooperation and information exchange, prompts the search for new methods and means of monitoring, detecting and neutralizing cyber threats, minimizing their consequences. Systemic risks are characterized by interconnectedness, spread in correlated systems, overcoming the limits of situational awareness or operational control. Risks are especially dangerous in the electric power industry, nuclear industry, aerospace companies, finance, state administration, etc. Systemic risk begins with a distributed vulnerability that changes as social and technological systems become more complex. The source of risk can be dependence of interconnected systems on information and communication technologies that support a widening range of applications. A system risk can be used by an attacker to destabilize or destroy critical functions. Individual initiating incidents accumulate and lead to undesirable effects that intensify with increasing damage. As a result, there are cascading effects that can affect both individual corporate information systems and the digital infrastructure of one or more sectors of economy.

Attacks come from a variety of sources and include denial of service attacks, the spread of malicious viruses that infect a critical infrastructure facility's network and use security breaches to access sensitive information, and spoofed emails requesting sensitive data from an unsuspecting employee, phishing.

Especially often, attackers are now using the capabilities of Artificial Intelligence. Thus, the ChatGPT language application is able to provide ready-to-use information from the Internet at the user's request. Thus, it significantly speeds up the process of knowledge of the criminal sphere, ordering large volumes of meaningful information. Obviously, this gives attackers the opportunity to significantly better prepare and subsequently commit encroachments of various types. In addition to the above, ChatGPT is able to create code in different programming languages, which opens up unlimited possibilities for cybercrime[10]. With the current version of the application, you can already create basic tools for a variety of malicious purposes — phishing pages, database hacking, etc.[11]

Simulation of a phishing attack includes detection and blocking by intrusion detection and computer attack prevention systems and antivirus software of electronic messages containing malicious code, reading them by computer users, and blocking the transmission of messages to attackers' servers. Attack vectors are built using computer automation tools. For this purpose, complete graph models of destructive



[10] Europol Tech Watch Flash. www.europol.europa.eu Retrieved from URL: https://www.europol. europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf[in English].

[11] 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.

cyber impacts on the network infrastructure of complex critical facilities can be developed.

Despite many methods of modeling information security threats and recognized registers or databases of software vulnerabilities, various systems for classifying and assessing the criticality of vulnerabilities, scientists often use only government databases as the main source of information about threats and vulnerabilities when developing a methodology for identifying the relationships between identified vulnerabilities of information systems and information security threats. This approach to assessing the irrelevance of the threat of unauthorized recovery of remote protected information for an information system by users authorized to access the information justifies the assumption that it is inexpedient to take actions to recover information already known to the offender and ignores the possibility of activating previously introduced malicious software code in this way.

Experimental methods based mainly on simulation (CyberVAN) and emulation (Testbed, INSALATA, SoftGrid and LARIAT), as well as methods of overlaying and demonstrating scenarios, help to overcome these difficulties. During the exercises, a multi-connected network (control centers, data centers) and attacks on information and operational technology systems via the Internet (SQL injections, Apache disconnections, NMS system destruction, database dump interception via file transfer protocol, ransomware, DDoS, SCADA, etc.) are often simulated.

In order to protect critical infrastructure from cyberattacks, we offer:

1. Modeling training environment by simulating cyber attacks

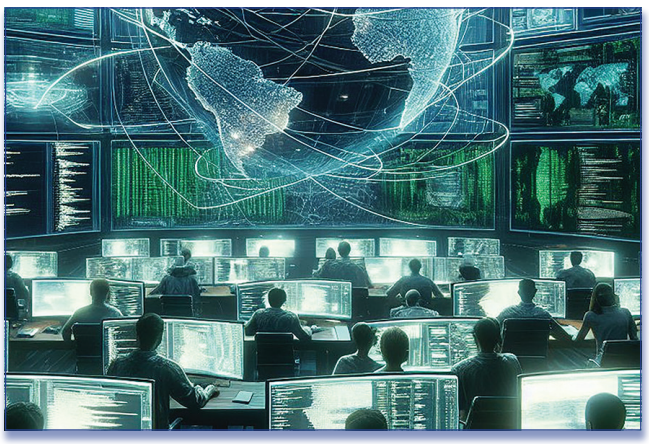
Every year, multi-step coordinated distributed cyberattacks with complex organization, implementation and multiple goals change, are conducted more often and more sophisticated. During the invasion phase, cyberattacks are usually detected using signature, behavioral, combined, and other methods. In the modern landscape of cyber-terrorist threats, creation of intelligent defenses that allow detecting targeted attacks at the initial stages of their implementation is coming to the fore.

Distinctive feature of critical infrastructure is its functioning through interaction with the global cyberspace, which creates additional vulnerabilities for possible exploitation in the course of destructive impacts on state and municipal systems and economic entities without direct penetration of the territory of the state and imposition of sanctions. In cyberspace, it is possible to remotely control and switch to a mode of operation in the interests of the perpetrator up to malfunctions of automated information systems and shutdown of critical infrastructure facilities. Putting a facility into emergency mode, which leads to its destruction, is particularly dangerous. When conducting exercises in cyberspace, modeling cyberterrorist attacks is an important stage of their preparation. The simulation is based on the formalization of a logical chain: the interaction of sets of identified software vulnerabilities, relevant threats, probable scenarios of threats, possible cyber-physical consequences, and quantitative assessment of cybersecurity risks.

Analysis of foreign experience in conducting cyber-terrorist exercises

In recent years, cyber-attackers have demonstrated readiness for cyber-activity against critical infrastructure facilities and aerospace industry enterprises through the use of resources and software available on the Internet.

Cybersecurity as an ever-expanding and exacerbating problem encompasses a combi-



O. Lytvynov, N. Filipenko, H. Spitsyna, A. Ivanović

CYBERPOLIGON – PRAKTYKA OCHRONY OBIEKTÓW INFRASTRUKTURY KRYTYCZNEJ I PRZEDSIĘBIORSTW PRZEMYSŁU LOTNICZEGO PRZED CYBERATAKAMI TERRORYSTYCZNYMI – DOŚWIADCZENIA UKRAINY I ŚWIATA (artykuł przeglądowy)

Streszczenie. Artykuł dotyczy kwestii opracowania i wdrożenia zestawu środków zapewniających bezpieczeństwo informacji i cyberterroryzmu w obiektach infrastruktury krytycznej i przedsiębiorstwach lotniczych wraz z opracowaniem środków przeciwdziałania hybrydowym wpływom przestępczym. Autorzy proponują utworzenie poligonów cybernetycznych, które dają możliwość badania złożonych ataków cyberterrorystycznych i szkolenia specjalistów ds. cyberbezpieczeństwa.

Autor analizuje zagraniczne doświadczenia w modelowaniu ataków cyberterrorystycznych podczas zakrojonych na szeroką skalę ćwiczeń cybernetycznych, które można wykorzystać do opracowania scenariuszy ataków cybernetycznych na krajowych poligonach cybernetycznych w celu szkolenia specjalistów w kontekście szybkiego rozwoju technologicznego i rosnących zagrożeń dla cyberbezpieczeństwa. Na podstawie uogólnionych doświadczeń zaproponowano taktyczne i organizacyjne środki zapobiegania atakom cyberterrorystycznym na obiekty infrastruktury krytycznej i przedsiębiorstwa lotnicze.

Słowa kluczowe: obiekty infrastruktury krytycznej, przedsiębiorstwa przemysłu lotniczego, poligony cybernetyczne, zagrożenia cyberterrorystyczne, cyberbezpieczeństwo.

nation of physical, software and human systems. A number of events are organized around the world to develop a training platform. Trainings play a key role in the formation and verification of organizational and technical readiness to repel real cyberattacks.

According to experts[12], the Cybersecurity Defense Initiative (CDI) program in the United States promotes comprehensive cybersecurity training for technical specialists, and courses are provided free of charge. The courses: Comprehensive Cybersecurity Defense and Cybersecurity Rapid Response Specialist are certified by the U.S. Department of Homeland Security. The U.S. Secret Service (USSS), with the participation of law enforcement agencies and private sector partners, conducts training on responding to cybersecurity incidents and developing mitigation strategies by virtually simulating attacks using ransomware and cryptocurrency. The FEMA Region III cybersecurity seminars include a presentation of the incident response plan and staff training. The FedVTE virtual cybersecurity training environment, managed by DHS, is available to employees of the federal government and other government agencies and government contractors on a free online platform. The environment, which is available on demand, contains modules for incident monitoring, risk management, and malware analysis. Federal departments use Einstein and US-Cert intrusion detection systems. In order to protect against malware attacks when connecting to federal systems, DHS is taking steps to reduce the number of Internet access points[13].

The current cyber-terrorist model can be developed for individual systems, networks and information and telecommunication infrastructure on which they operate. Threats associated with interfaces with systems and networks are initiated during development of training episodes by proving the inputs.

Modeling cyberterrorist attacks includes determining possible negative consequences of their implementation, conditions of implementation and sources of threats, assessment of attackers' capabilities, scenarios of threats and danger of cyberattacks. The goals and scenarios of threats and the predicted consequences of their implementation are specified by an expert method. Critical communications and energy supply systems are considered so important to the United States that their disruption or destruction could have a detrimental impact on various types of security: national, economic, and public. Officials recognize that eliminating the consequences of deliberate cyberattacks on critical infrastructures is costly for the country[14]. Therefore, to solve systemic problems, prioritization, development of common terminology, and organization of incident response are needed.

Conclusions. The state of security of critical infrastructure and aerospace enterprises is an integral part of Ukraine's

[12] Див. докладніше: Thakur K, Ali ML, Jiang N et al. Impact of cyber-attacks on critical infrastructure. In: 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016. New York, NY, USA.Kavak H., Padilla J.J., Vernon-Bido D., Diallo S.Y., Gore R.J., Shetty S. Simulation for Cybersecurity: State of the Art and Future Directions. Journal of Cybersecurity, Volume 7, Issue 1, 2021. DOI: 10.1093/cybsec/tyab005

[13] Kavak H., Padilla J.J., Vernon-Bido D., Diallo S.Y., Gore R.J., Shetty S. Simulation for Cybersecurity: State of the Art and Future Directions. Journal of Cybersecurity, Volume 7, Issue 1, 2021. DOI: 10.1093/cybsec/tyab005

[14] CISA, Cyber Storm VI: National Cyber Exercise, D.o.H. Security, Editor, 2020. URL: http://www.cisa.gov/cyber-storm-vi

national security. Currently, there is an acute problem of financing and logistical support for those facilities that have suffered as a result of military operations. As a matter of urgency, the regulatory acts related to the creation of effective conditions for the functioning and restoration of critical infrastructure during martial law were promptly finalized. This issue is fundamental in the process of developing productive mechanisms to ensure the national security interests of our country. In this regard, further scientific study is required to adapt international experience in protecting and enhancing the resilience of critical infrastructure, in particular in the context of military threats. It should be taken into account that effective implementation of measures to protect critical infrastructure will require the integration of new technologies, implementation of innovative solutions and development of cooperation between government agencies and private companies. This will not only restore damaged facilities but also significantly strengthen their resilience to potential threats in the future.

For this purpose, it is proposed:

Firstly, create an extensive system of public and private cyber polygons that will allow:

1. Explore real-world cyber terrorist attack scenarios: Training ranges will simulate different types of attacks, from DDoS attacks to phishing and data theft. This will enable researchers and cybersecurity professionals to study adversary behavior, develop new security techniques, and improve existing security systems.

2. Train highly qualified specialists: cyber training will allow future cybersecurity specialists to acquire the practical skills necessary to work in the real world. They will be able to practice different scenarios, develop analytical skills and improve their skills in responding to cyber threats.

3. Develop automated monitoring methods: with the help of artificial intelligence and machine learning, it is possible to create systems that will automatically detect suspicious activity on the network.

4. Improve analytical information processing tools: analysis of large amounts of data will identify trends and patterns of cyber-terrorist attacks on critical infrastructure facilities and aerospace enterprises, which will help in predicting and preventing future incidents.

5. Create forecasting and planning systems: through data analysis and modeling, it will be possible to predict future cyber threats and develop plans for their neutralization.

6. Ensure effective counteraction to information threats: cyber training will develop strategies for passive and active counteraction to cyber terrorist attacks, including the development of new technologies for protection and improvement of existing security systems.

Creation of cyber polygons is a key step for ensuring cybersecurity in the modern world. This will prepare a new generation of cybersecurity specialists, develop effective methods of protection and ensure the security of information systems from cyberattacks.

Secondly, in order to prevent cyber-terrorist attacks on critical infrastructure facilities and enterprises of the aerospace industry, we offer:

1. Strengthen the cybersecurity of public and private enterprises: Implement multi-factor authentication (MFA) for all users and administrators. Update software and operating systems regularly to address known vulnerabilities. Apply intru-

sion detection and prevention systems (IDS/IPS) to monitor network traffic and block suspicious activity. Establish a data backup and disaster recovery system to minimize damage from cyberattacks. Conduct regular staff training on cyber security and safe use of Internet.

2. Improve cooperation between public authorities: Report suspicious cyber threats and incidents to the relevant authorities. Participate in joint cybersecurity exercises and trainings. Facilitate the development and implementation of national cybersecurity standards.

3. Engage private sector: Create a platform to share information on cyber threats and best practices. Encourage investment in the development and implementation of innovative cybersecurity solutions. Collaborate with research institutions to develop new technologies to protect against cyberattacks.

4. Increase public awareness: Conduct information campaigns about cybersecurity threats and ways to protect. Teach children and young people the basics of cybersecurity. Create online resources with cybersecurity information and protection recommendations.

Application of these measures will help to significantly increase the level of cybersecurity of critical infrastructure facilities and aerospace enterprises and minimize the risks of cyber-terrorist attacks.

References

Batyrhareyeva, V. S., Babenko, A. M. (2020). Analiz suchasnoyi kryminohennoyi sytuatsiyi v Ukrayini yak informatsiyna model' dlya rozrobky stratehiyi zmenshennya mozhlyvostey vchynennya zlochyniv. *Arkhiv kryminolohiyi ta sudovykh nauk* : nauk. zhurnal. Kharkiv : KHNDISE, No. 1. C 39–53. [in Ukrainian].

CISA, Cyber Storm VI: National Cyber Exercise, D.o.H. Security, Editor, 2020. URL: http://www.cisa.gov/cyber-storm-vi [in English].

Danyk, YU.H. (2019). Osoblyvosti stvorennya kiberpolihoniv dlya doslidzhennya kompleksnykh kiberdiy ta pidhotovky fakhivtsiv z kiberbezpeky. Confrontation in the cybernetic. *Modern Information Technologies in the Sphere of Security and Defence* № 1(34)/2019. DOI:10.33099/2311-7249/2019-34-1-95-102. [in Ukrainian].

Europol Tech Watch Flash. www.europol.europa.eu Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf [in English].

Filipenko, N. (2022). Protydiya kiberatakam na ob'yekty krytychnoyi infrastruktury ta zhyttyezabezpechennya pid chas viys'kovoyi ahresiyi proty Ukrayiny. Ukrayins'kyy doslidnyts'kyy prostir v umovakh viyny: adaptatsiya y perezavantazhennya tekhnichnykh i yurydychnykh nauk: zbirnyk materialiv dopovidey uchasnykiv mizhnarodnoyi naukovo-praktychnoyi konferentsiyi. (Kharkiv-Ryha, 31 travnya 2022 r.). Kharkiv, 2022. Pp. 213-217. [in Ukrainian].

Filipenko, N. YE., Lukashevych, S. YU. (2023). Informatsiyni metodyky doslidzhennya kryminal'nykh pravoporushen', vchynenykh z vykorystannyam tekhnolohiy shtuchnoho intelektu. *Naukovi perspektyvy* (Seriya «Derzhavne upravlinnya», Seriya «Pravo», Seriya «Ekonomika», Seriya «Medytsyna», Seriya «Pedahohika», Seriya «Psykholohiya») Vypusk № 11(41)2023. Kyiv. № 1(7) C.1084-1096. [in Ukrainian].

Kavak, H., Padilla, J.J., Vernon-Bido, D., Diallo, S. Y., Gore, R. J., Shetty, S. (2021). Simulation for Cybersecurity: State of the Art and Future Directions. J*ournal of Cybersecurity,* Volume 7, Issue 1. DOI: 10.1093/cybsec/tyab005 [in English].

Kuz'menko, YU. V., Koropatov, O. M., Dumans'kyy, R. V. (2022). Administratyvno-pravove zabezpechennya zakhystu ob`yektiv krytychnoyi infrastruktury Ukrayiny pid chas voyennoho stanu. *Yurydychnyy Byuleten*'. Vypusk 27. DOI https://doi.org/10.32850/LB2414-4207.2022.27.08 . [in Ukrainian].

Kuz'menko, YU. V., Bondar,V. V. (2021). Zakhyst ob`yektiv krytychnoyi infrastruktury: administratyvno-pravove zabezpechennya. *Yurydychnyy byuleten'*. Vyp. 21. Pp. 67–72. [in Ukrainian].

Lallie, H. S., Shepherd, L. A., Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple, C., Bellekens ,X. (2021). Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers and Security*, 105, [102248]. URL: http://doi.org/10.1016/j.cose.2021.102248 [in English].

Leblanc, S. P., Partington, A., Chapman, I. M., Bernier, M. (2011). An overview of cyber attack and computer network operations simulation. SpringSim (MMS). Pp. 92–100. [in English].

Mykola Nechyporuk, Volodymyr Pavlikov, Nataliia Filipenko, Hanna Spitsyna, Ihor Shynkarenko, (2020). Cyberterrorism Attacks on Critical Infrastructure and Aviation: Criminal and Legal Policy of Countering. Integrated Computer Technologies in Mechanical Engineering — 2020. Synergetic Engineering P. 206–220. ISBN 978-3-030-66716-0 ISBN 978-3-030-66717-7 (eBook). URL: https://doi.org/10.1007/978-3-030-66717-7. [in English].

Natsional'nyy tsentr rezervuvannya derzhavnykh informatsiynykh resursiv (NTS). URL: https://uss.gov.ua/service/natsionalnyj-tsentr-rezervuvannya-derzhavnyh-informatsijnyh-resursiv-nts/#:~:text=За%20час%20повномасштабної%20війни%20кількість,а%20в%202021%20–%20близько%202000. [in Ukrainian].

Thakur, K., Ali, ML., Jiang, N. et al. (2016). Impact of cyber-attacks on critical infrastructure. In: 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS).New York, NY, USA. [in English].

VITI otrymav kiberpolihon. https://mil.in.ua/uk/news/viti-otrymav-kiberpoligon/ [in Ukrainian].

Yehor Aushev zapustyv kiberpolihon dlya trenuvannya spetsialistiv — tam vzhe ye ponad 150 stsenariyiv ataky i zakhystu. https://dou.ua/lenta/news/about-unit-range/ [in Ukrainian].

Received by Editorial Board: 16.08.2024

Suggested Citation:

Lytvynov, O., Filipenko, N., Spitsyna, H., Ivanović, A. (2024). Cyber Polygon — Practice of Protecting Critical Infrastructure Objects and Companies of Aviation Industry from Cyber Terrorist Attacks — Experience of Ukraine and the World (Review article). *Archives of Criminology and Forensic Sciences*. 2 (10). 50-59. DOI: https://doi.org/10.32353/acfs.10.2024.01