СЕРІЯ «Право»

UDC 004.056

https://doi.org/10.52058/2786-5274-2023-11(25)-197-205

Haborets Olha Andriivna PhD in Pedagogical Sciences, Associate Professor of the Department of Operational-Search Activities and Information Security, Donetsk State University of Internal Affairs, Kropyvnytskyi, https://orcid.org/0000-0001-7791-6795

ENSURING CYBERSECURITY OF UKRAINE AGAINST CYBERTERRORISM THREATS: A SYSTEMATIC APPROACH

Abstract. The escalating landscape of cyber threats and cyberterrorism prompts a critical examination of Ukraine's cybersecurity preparedness. This paper investigates the multifaceted dimensions of Ukraine's cybersecurity challenges, notably in countering cyberterrorism. The evolution of cyber incidents since 2014, coupled with recent surges in cyberattacks, underscores the pressing need for a comprehensive approach.

The paper delves into the imperative of public-private partnerships, emphasizing information exchange, expert involvement, and adherence to international conventions. Challenges stemming from procedural uncertainties, and limited cybersecurity education are highlighted. The necessity of a national program for securing critical information infrastructure is stressed, along with the adoption of international standards, continuous vulnerability assessment, and emergency response planning.

The discussion encompasses the significance of cybersecurity audits, software certification, and indigenous technology development. Amid the quest for digital sovereignty, a dedicated domestic technology program emerges as vital. The paper's findings advocate for a systematic, comprehensive, and sustainable approach to cybersecurity in Ukraine, ultimately strengthening its resilience against evolving cyber threats.

By encapsulating these principles and measures, Ukraine can fortify its cybersecurity defenses, effectively counter cyber challenges, and safeguard its national interests. In the face of escalating cyber threats, it is imperative for Ukraine to address the interconnected nature of cyber and military actions. This calls for concerted efforts to enhance digital literacy, develop resilient indigenous technologies, and foster international collaborations. As Ukraine navigates its path towards digital sovereignty, a proactive cybersecurity strategy is paramount for

safeguarding critical infrastructure, bolstering national security, and ensuring a cyber-resilient future.

Keywords: cybersecurity, cyber threats, cyberterrorism, public-private partnership, critical infrastructure, cyber incidents, National program, International standards.

Габорець Ольга Андріївна, доктор філософії, доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки, Донецький державний університет внутрішніх справ, м. Кропивницький, https://orcid.org/0000-0001-7791-6795

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ ВІД ЗАГРОЗ КІБЕРТЕРРОРИЗМУ: СИСТЕМНИЙ ПІДХІД

Анотація. Ескалація кіберзагроз і кібертероризму спонукає до критичного аналізу готовності України до кібербезпеки. У цій статті досліджуються багатогранні виміри викликів кібербезпеці України, зокрема у сфері протидії кібертероризму. Еволюція кіберінцидентів з 2014 року в поєднанні з нещодавніми сплесками кібератак підкреслює гостру потребу в комплексному підході.

У документі розглядається імператив державно-приватного партнерства, наголошується на обміні інформацією, залученні експертів та дотриманні міжнародних конвенцій. Висвітлено проблеми, пов’язані з процедурною невизначеністю та обмеженою освітою з питань кібербезпеки. Наголошується на необхідності національної програми забезпечення безпеки критичної інформаційної інфраструктури, а також прийняття міжнародних стандартів, постійної оцінки вразливості та планування реагування на надзвичайні ситуації.

Обговорення охоплює важливість аудитів кібербезпеки, сертифікації програмного забезпечення та розвитку місцевих технологій. Серед прагнення до цифрового суверенітету життєво важливою стає спеціальна програма внутрішніх технологій. Висновки, зроблені в документі, свідчать про систематичний, комплексний і стійкий підхід до кібербезпеки в Україні, що в кінцевому підсумку посилить її стійкість проти нових кіберзагроз.

Впроваджуючи ці принципи та заходи, Україна може зміцнити захист своєї кібербезпеки, ефективно протидіяти кібервикликам і захистити свої національні інтереси. В умовах ескалації кіберзагроз Україні вкрай необхідно звернути увагу на взаємопов’язаний характер кібернетичних і військових дій. Це вимагає узгоджених зусиль для підвищення цифрової грамотності, розвитку стійких місцевих технологій і сприяння міжнародній співпраці. Оскільки Україна рухається своїм шляхом до цифрового суверенітету, проактивна стратегія кібербезпеки має першорядне значення для захисту критичної інфраструктури, зміцнення національної безпеки та забезпечення кіберстійкого майбутнього.

Ключові слова: кібербезпека, кіберзагрози, кібертероризм, державно-приватне партнерство, критична інфраструктура, кіберінциденти, Національна програма, Міжнародні стандарти.

Statement of the problem. Cybersecurity has emerged as a critical concern in today's interconnected world, where technological advancements have revolutionized various aspects of society. Ukraine, like many other nations, faces escalating cyberterrorism threats that pose significant risks to its national security, economy, and public safety. Addressing these threats requires a comprehensive and systematic approach to ensure the cybersecurity of the country.

The purpose of this paper is to explore the topic of ensuring cybersecurity in Ukraine, specifically focusing on the growing challenges posed by cyberterrorism. Cyberterrorism refers to the malicious use of technology to instigate fear, disrupt critical infrastructure, and harm individuals or institutions. As Ukraine increasingly relies on digital systems for various sectors such as government operations, finance, energy, and transportation, the vulnerability to cyberterrorism becomes a pressing issue.

To counter these threats effectively, a systematic approach is necessary. This approach involves implementing robust policies, developing advanced technological capabilities, fostering international cooperation, and enhancing the capacity of cybersecurity professionals. By adopting a comprehensive strategy that encompasses prevention, detection, response, and recovery, Ukraine can fortify its cyber defenses and mitigate the impact of cyberterrorism incidents.

This paper will delve into various aspects of ensuring cybersecurity against cyberterrorism threats in Ukraine. It will examine the current landscape of cyber threats faced by the country, analyze the potential consequences of cyberterrorism, and explore the systemic approach required to safeguard critical systems and infrastructure. Additionally, the paper will highlight the importance of collaboration between government agencies, private sector entities, and international partners to strengthen Ukraine's cybersecurity posture.

An example of the basic material.

Cyber-attacks against Ukraine have a longstanding history, dating back to 2014, when Russia annexed Crimea and occupied parts of the Donbas region. Since then, Ukraine has faced numerous cyber incidents, becoming a testing ground for state-of-the-art cyber weapons. Notable milestones include cyber-attacks on the Ukrainian election system in 2014, energy blackouts in 2015, and the Petya ransomware attack in 2017. These incidents have highlighted the importance of bolstering Ukraine's cybersecurity defenses and preparedness to counter future threats effectively.

Recently, cyber experts have observed a significant surge in cyber incidents starting from mid-2021, and this trend further escalated leading up to Russia's full-scale invasion in early 2022. Statistics from Ukraine's National Computer

Emergency Response Team Cert-UA indicate that the number of attacks witnessed a nearly tenfold increase in the first months of 2022 compared to the previous year. The rise in cyber threats has become a pressing concern, necessitating heightened vigilance and proactive measures to bolster Ukraine's cybersecurity defenses in the face of escalating cyber challenges.

Numerous experts accurately anticipated that kinetic military actions in Ukraine would coincide with extensive cyber operations. The Russian invasion of Ukraine has highlighted the interconnected nature of simultaneous threats faced by businesses and governments. These threats encompass nation-backed cyber-attacks targeting local IT systems and infrastructure, alongside traditional military actions resulting from the ongoing conflict.

Since the start of Russia's full-scale war in February 2022, Ukraine has experienced a barrage of cyber-attacks impacting public institutions, private organizations, and individual citizens. These attacks have specifically targeted critical infrastructure sectors, including energy, telecommunications, media, and financial entities.

This unfolding situation underscores the imperative for businesses and governments to recognize the inseparable link between cyber threats and traditional military actions. It calls for heightened efforts to safeguard against cyber-attacks on vital systems, protect national interests, and bolster overall cybersecurity defenses during times of conflict.

Considerable attention should be directed towards information security to preempt the actions of state aggressors regarding the deployment of information, hybrid, network-centric warfare, and the like. In the military doctrines of NATO countries, the promotion of democratic ideals is highlighted as the foremost task of their Armed Forces. This is due to the increasing importance of prioritizing spiritual substance over material substance in the process of organizing their cyber defense efforts.

Unfortunately, Ukraine's current legislation on cybersecurity lacks clear hierarchical structure, unity, and comprehensiveness. This leads to conflicting interpretations and applications of its norms in practice. This issue arises, in part, because certain integral problems are addressed in different normative acts in a fragmented manner and without coordination among them [1].

Hence, the implementation of a comprehensive approach to ensuring Ukraine's information security in the context of hybrid warfare seems pertinent. This approach should encompass the following elements:

– formulating a "soft power" policy primarily focused on safeguarding, preserving, and nurturing spiritual values, including patriotic ones;

– developing principles of state information policy with a focus on information security in networked environments and social media platforms;

– transitioning from a reactive strategy towards information that is already disseminated in networked environments and the Internet, to a strategy of filling informational gaps with objective and high-quality information;

– establishing a dedicated DNS server and creating high-quality domestic software to address the issue of cyber security for critical infrastructure objects; (268)

– initiating the development and implementation of programs to enhance the knowledge of employees working in critical infrastructure sectors and the general population of the country regarding cybersecurity and cyber hygiene;

– collaborating with EU countries on matters pertaining to establishing a unified secure cyber space and ensuring overall cyber security.

Drawing from international experience, it would be advisable for Ukraine to consider the following actions:

– establish a state center for safeguarding critical infrastructure;

– enhance the institution of public-private partnership in the realm of cybersecurity, develop methods and types of state-private partnership initiatives to ensure cybersecurity, and regularly conduct cyber education for a range of Ukrainian government bodies responsible for critical infrastructure, aimed at countering cyber attacks;

– create a system (network) of Cyber Incident Response Teams (CERTs) that includes both national, local, and sector-specific centers. Presently, Ukraine has only one such center within its territory;

– minimize the reliance on foreign-produced software and hardware components, incentivize the growth of a domestic sector to enable the creation of proprietary operating systems, antivirus solutions, and telecommunications equipment. This emphasis is especially relevant for critical information infrastructure entities of the nation. In the extreme case, consider employing tools with open-source code and infrastructure to safeguard against concealed backdoors or other potential interventions in these tools by unauthorized entities.

A continuous and systematic exchange of data on current cyber threats and potential countermeasures is of paramount importance in this aspect. Therefore, it would be optimal to establish and sustain a comprehensive cybersecurity public-private partnership, forming a national data exchange system for cyber incident information and maintaining a registry of cyber incidents. This would empower cybersecurity units to scrutinize compromise markers, trace the distribution of similar malicious software, and share indicators of cyber attacks, thereby ensuring the effective protection of their entities against cyber attacks [1, p. 63].

By implementing these measures, Ukraine can fortify its cybersecurity posture and proactively counter emerging cyber threats.

In general, the following key directions can be highlighted in the field of public-private partnership in the process of ensuring cybersecurity [1, p. 55]:

– providing critical infrastructure owners and operators with information on detecting cyberattacks and/or cyber incidents, vulnerabilities in their cybersecurity systems;

– developing organizational and legal principles and directly involving experts from the private sector (including activists) in conducting covert assessments

of the preparedness of critical infrastructure objects for cyberattacks and cyber incidents;

– ensuring compliance by operators and providers of telecommunications with the provisions of the Council of Europe Convention on Cybercrime, regarding the urgent preservation and provision of data to competent law enforcement authorities necessary for countering cyberterrorism.

The absence of a legislatively regulated and financially supported strategy for public-private partnership in the field of cybersecurity, unresolved procedural issues concerning the actions of law enforcement and regulatory authorities in this field, uncertainty in the distribution of responsibilities between governmental and private institutions in the cybersecurity sphere, as well as inadequate attention to issues of general cybersecurity education, raising public awareness, and enhancing the technological potential for cybersecurity, significantly increase Ukraine's vulnerability to cyber incidents and cyber attacks.

To establish effective cybersecurity for critical infrastructure objects in Ukraine, it is advisable to develop a comprehensive set of measures aimed at creating a national system to ensure the security of strategically important national critical objects, including information infrastructure, based on a unified methodological approach for identifying critical objects and selecting methods and tools to enhance their protection against cyber threats.

In Ukraine, a pressing task is the development of a national program that ensures the cybersecurity of critically important information infrastructures of the country.

To assess the security of information systems, we propose implementing cybersecurity audits in accordance with international standards. Such audits should be conducted regularly, involving independent experts, preferably external, who possess international certification.

However, at present, there exists an issue of low-quality cybersecurity audits, as only government-accredited organizations have permission to conduct them. International certificates in information security and IT auditing are not currently recognized, which adversely affects the quality of cybersecurity audits.

Moreover, due to the specifics of many sectors (healthcare, energy, telecommunications, etc.), there is a pressing need to implement industry-specific cybersecurity standards. Overall, the transition to international cybersecurity standards, including sector-specific ones, is necessary for the country. A range of international standards such as NIST, ISO, and Cobit have proven themselves in developed countries and stood the test of time.

Alongside this, continuous analysis and monitoring of vulnerabilities in information systems across various sectors of critical infrastructure are essential. This task gained particular importance during the COVID-19 pandemic when remote access to internal information resources of enterprises was provided via the Internet to enable remote work for certain employees.

Furthermore, an integral part of ensuring cybersecurity for critical information infrastructure systems is the development of an action plan for emergencies and a regimen for managing cyber incidents.

All these measures can be laid out in the State-approved Cybersecurity Strategy for Key Information Infrastructure Systems of the country, which includes organizational, technical, and regulatory measures, methods, and means for protecting critical information.

In general, the following principles should be applied to ensure protection against cyber threats, including cyber terrorism, for critical information infrastructure:

– the approach to ensuring cybersecurity and cyber protection of critical information infrastructure should be systematic (comprehensive);

– the process of enhancing and developing cybersecurity and cyber protection for critical information infrastructure should be continuous and realized through rational methods, approaches, and measures based on the requirements of current legislation, relevant national and international standards for cybersecurity, and the best foreign practices;

– measures to protect against real and potential cyber threats to critical information infrastructure should be timely and adequate;

– sustainable development of critical information infrastructure cybersecurity systems is possible only if sufficient resources, including financial ones, are provided.

One of the tasks of ensuring cybersecurity in Ukraine is also the certification of foreign software before its transfer to government agencies. Sometimes, hidden vulnerabilities are discovered in the programs, hence one of the ways to counter such cyber threats is to conduct security assessments of the software code during the certification trials.

In the context of the necessity to strengthen Ukraine's digital sovereignty, it is crucial to have a dedicated program for developing its own information technologies based on domestic advancements in fundamental science. This is aimed at effectively countering cyber attacks.

Certainly, here are further elaborated steps that can be taken across the conceptual, regulatory, and institutional dimensions to form a robust system for countering cybercrime, particularly cyberterrorism, in Ukraine:

Conceptual Dimension:

National Cybersecurity Strategy: Develop a comprehensive national cybersecurity strategy that outlines clear objectives, priorities, and action plans to address various cyber threats, including cyberterrorism. This strategy should be regularly updated to stay ahead of evolving threats.

Public Awareness and Education: Launch public awareness campaigns to educate citizens about the risks of cybercrime and cyberterrorism. Promote responsible online behavior, digital hygiene, and the importance of reporting suspicious activities.

International Cooperation: Strengthen collaborations with international partners, including sharing threat intelligence, participating in joint cyber exercises, and establishing bilateral/multilateral agreements to enhance cyber resilience and response capabilities.

Regulatory and Legal Dimension:

Cybercrime Legislation: Enact and regularly update comprehensive cybercrime laws that define cyber offenses, establish penalties, and provide legal mechanisms for investigating and prosecuting cybercriminals. These laws should be in line with international standards and conventions.

Data Protection and Privacy Laws: Strengthen data protection and privacy regulations to safeguard personal and sensitive information from cyber threats. Ensure that individuals' rights are protected and that organizations implement adequate security measures to prevent data breaches.

Incident Reporting Framework: Establish a mandatory incident reporting framework that requires organizations to report cyber incidents to relevant authorities. This facilitates early detection, information sharing, and a coordinated response.

Cross-Border Jurisdiction: Address challenges related to cross-border cybercrime by formulating legal mechanisms for extraditing cybercriminals, facilitating international cooperation in investigations, and harmonizing legal processes.

Institutional Dimension:

Cybersecurity Agency: Create a dedicated national cybersecurity agency responsible for coordinating and implementing cybersecurity strategies, policies, and initiatives. This agency should have authority over cybersecurity matters across various sectors.

Capacity Building: Invest in training programs for law enforcement agencies, judiciary, and prosecutors to enhance their understanding of cybercrimes and cyberterrorism. Equip them with the skills needed to investigate, prosecute, and adjudicate cyber-related cases.

Public-Private Partnerships: Foster collaboration between government agencies, private sector entities, academia, and research institutions. Encourage information sharing, joint research, and the development of cybersecurity technologies and solutions.

Rapid Response Teams: Establish specialized cybersecurity response teams that can be activated in the event of a cyber incident. These teams should be trained to handle emergencies, conduct digital forensics, and mitigate threats.

Certification and Standards: Develop cybersecurity standards and certification programs for critical sectors like energy, finance, healthcare, and transportation. This ensures that organizations adhere to minimum security requirements.

By implementing a multifaceted approach across these dimensions, Ukraine can build a resilient and effective system to counter cybercrime, protect critical infrastructure, and mitigate the risks associated with cyberterrorism.

Conclusions. Approaching the issue of cyberterrorism prevention holistically, the emphasis should be placed on the importance of not only focusing on cybersecurity policy at the national level, but also on the administrative and lower yet equally vital levels. Cyber protection must be implemented at the operational level while executing a unified security policy across the Internet networks.

Operational regulators should primarily prioritize individuals and ensure the reduction of damages caused by cyberattacks through timely responses, efficient operations, and quality recovery. Additionally, each corporate employee should possess minimal privileges necessary for fulfilling their duties.

As a result, even if an attacker manages to infiltrate any company, they won't be able to cause significant harm.

References:

1. Dubov D. (Ed.). (2018). Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky: mizhnarodnyi dosvid ta mozhlyvosti dlia Ukrainy [Public-private partnership in the field of cyber security: international experience and capabilities for Ukraine]. Kyiv: NISD [in Ukrainian].

Література:

1. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можтвості для України: аналіт. дол. / за заг. ред. Д. Дубова. К.: НІСД, 2018. 84 с. С. 63.