SECURITY THINKING: THE UKRAINIAN CONTEXT

Oleksandra Liashenko[1]

[1]Doctor of Science (Economics), Professor, Management and Organization Development Department, Ukrainian Catholic University, Lviv, Ukraine, e-mail: Lan911@ukr.net, ORCID: https://orcid.org/0000-0001-7114-4501

Citation:
Liashenko, O. (2023). Security thinking: the Ukrainian context. *Economics, Finance and Management Review*, (2), 137–146. https://doi.org/10.36690/2674-5208-2023-2-137-146

Received: June 01, 2023
Approved: June 28, 2023
Published: June 30, 2023

Abstract. *In an increasingly interconnected world, the security landscape has become exponentially more complex. Organizations and individuals face a myriad of threats, from sophisticated attacks to ever-evolving vulnerabilities. In order to successfully navigate this treacherous terrain, it is critical to develop a safety-focused mindset. Taking this proactive approach can pave the way for resilience to complexity, where strong defenses and adaptive strategies work in tandem to protect our security ecosystem. Security Thinking is a proactive approach to analyzing and addressing potential risks and vulnerabilities in order to enhance security measures. It involves a mindset that prioritizes prevention, preparedness, and adaptability to protect against various threats and challenges. Security Thinking encourages individuals and organizations to consider security implications at every level, from technology and processes to human behavior, promoting a resilient and secure environment. It is a continuous and dynamic process that seeks to stay ahead of emerging threats and evolve in response to changing security landscapes. At the same time, there is another definition. Security Mindset is an individual's or organization's way of thinking that places a strong emphasis on security and risk management. It involves being proactive in identifying potential threats, vulnerabilities, and weaknesses in systems, processes, and behaviors. Developing a security mindset is not an end point, but a continuous journey. Using intellectual rigor and an innovative spirit, you can significantly influence the formation of a security ecosystem. The principles of resilience to complexity and a holistic approach to security, guided by a security-centric mindset, are becoming a dynamic force in protecting the security ecosystem. By integrating physical security, modernized legislation, social engineering, data privacy protection and psychological security, we can build a fortress against a wide range of threats. However, the unprecedented challenges associated with Russia's full-scale war against Ukraine have significantly complicated the architecture of modern security, creating a need for the development of a new paradigm of security thinking and practical tools for its application.*

Keywords*: security thinking; security mindset; security landscape.*
JEL Classification: H 56
Formulas: 0; fig.: 2; tabl.: 1; bibl.: 17

Introduction. In an increasingly interconnected world, the security landscape has become exponentially more complex. Organizations and individuals face a myriad of threats, from sophisticated attacks to ever-evolving vulnerabilities. In order to successfully navigate this treacherous terrain, it is critical to develop a safety-focused mindset. Taking this proactive approach can pave the way for resilience to complexity, where strong defenses and adaptive strategies work in tandem to protect our security ecosystem. A dynamic security environment is one that is constantly changing and evolving, requiring security measures to be constantly updated and adapted to keep pace with new threats and risks. Such an environment can be characterized by a range of factors, including:

Emergence of new threats: A dynamic security environment is often characterized by the emergence of new threats that were not present or well understood previously. These threats can come from a range of sources, such as cyberattacks, terrorism, natural disasters, or geopolitical risks.

Rapid technological change: Technology is constantly advancing and changing, which means that security measures must also adapt and evolve to keep pace. This can include everything from new software and hardware systems to emerging trends in social media and other digital platforms.

Increased interconnectedness: As the world becomes more interconnected, the risks associated with various systems and networks can quickly multiply. A dynamic security environment may include a range of interconnected systems, such as transportation networks, financial systems, and critical infrastructure.

Evolving threat actors: Threat actors, such as hackers, cybercriminals, and terrorists, are constantly evolving their tactics and techniques. A dynamic security environment requires security measures that are able to detect and respond to these new threats in real-time.

Heightened uncertainty: A dynamic security environment can be characterized by heightened uncertainty, where risks and threats may be difficult to predict or quantify. This can make it challenging to develop effective security measures that are able to address these risks in a proactive and strategic way.

Literature review. In the modern era of globalization changes, with the development of information civilization, security science is becoming more and more important. The interdisciplinary direction is today the main advantage and the base that constantly creates and multiplies the overall potential of a person, the state and society. After all, the modern world; we live in jasper, permeated with all social troubles, cataclysms, and also full of military conflicts. That is why the urgent need and interest of each of us in the study of the interdisciplinary science Security Studies requires. At the same time, it is worth noting that consciousness, language, and preventive instructions of wisdom must serve as constructions in security science. [1, 2].

The theory of securitization, proposed by B. Buzan, O. Waever, and other representatives of the Copenhagen School, has allowed for an expanded understanding of the concept of security. This includes not only military aspects but also political, economic, social, and environmental components. The scientific community recognized the crucial role of the state in ensuring national security [3]. In the 1994 Human Development Report, a new scientific concept prioritizing human security and its constituent elements – economic security, food security, health security, environmental security, personal security, community security, and political security – was formulated based on the conclusion that achieving world peace necessitates individual safety in daily life [4]. D. Held and A. McGrew argue that globalization has led to a shift from state-centric policies to a new complex form of multilayered global governance in security provision. While different states have gained varying benefits from globalization based on their potential and level of development, there is an overall trend towards reduced capabilities of national states to ensure security due to lack of institutional capacity [5]. Subsequently, global leaders moved towards forming a "global community" and developing the concept of human security prioritization. D. Chandler analyzed the paradigm shift in security studies [6]. However, the concept of responsibility for global security by "strong" states and their right to intervene in the internal affairs of other states (supposedly to protect basic human rights) proved to be problematic in practice, creating fundamental contradictions between this right and the sovereign rights of independent states. Indeed, this can characterize Russia's behavior towards Ukraine as a distortion of the security paradigm. Additionally, the necessary measures in the field of global security required proper resource provisioning and became quite burdensome for the economies of "strong" states. Changes in the global security environment, the emergence of new and the intensification of traditional threats, have brought forward questions regarding the development of security thinking. In Ukraine, this process is just beginning, while at the same time, it is establishing new frameworks for such thinking on a global scale.

Security Revolution. Long-standing norms and security systems are being challenged in a variety of ways. Existing structures have so far been sufficient to meet the new challenges, but signs of stress in the security system are growing. Thanks to 21st century technologies – from communications to munitions – the means of breaching security are becoming cheaper, easier to find and use. Structures built to deal with 20th century problems are struggling to cope with 21st century technologies that are moving faster than problem management systems can adapt. Transnational Threats: The time it takes for a threat to move from one territory to another has been reduced by orders of magnitude. Pervasiveness and mutating threats: A connected world creates great opportunities for individual human advancement, but also risks entirely new forms of vulnerability. There are dozens of potential sources for this topic, depending on what specific areas of security need to be studied. Potential options are the CSIS Annual Global Security Outlook and SIPRI's Peace and Security Publications.

Aims. Creating a paradigm of security thinking with consideration of the context of the Russian Federation's war against Ukraine.

Methodology. *Security Thinking* is a proactive approach to analyzing and addressing potential risks and vulnerabilities in order to enhance security measures. It involves a mindset that prioritizes prevention, preparedness, and adaptability to protect against various threats and challenges. Security Thinking encourages individuals and organizations to consider security implications at every level, from technology and processes to human behavior, promoting a resilient and secure environment. It is a continuous and dynamic process that seeks to stay ahead of emerging threats and evolve in response to changing security landscapes. At the same time, there is another definition.

Security Mindset is an individual's or organization's way of thinking that places a strong emphasis on security and risk management. It involves being proactive in identifying potential threats, vulnerabilities, and weaknesses in systems, processes, and behaviors. Having a Security Mindset means being vigilant, cautious, and conscious of security implications in all activities. Key characteristics of a Security Mindset include next characteristics. Awareness: Being aware of the potential risks and threats that exist in various environments, including physical, digital, and social spaces. Proactivity: Taking proactive measures to prevent security breaches and implementing preemptive security measures to minimize vulnerabilities. Adaptability: Being able to adjust and respond to new and emerging security threats and challenges effectively. Continuous Learning: Engaging in ongoing education and training to stay updated on the latest security trends, technologies, and best practices. Risk Assessment: Conducting regular risk assessments to identify and prioritize potential security risks and develop mitigation strategies. Responsibility: Taking personal responsibility for security, whether it's securing personal devices or following security protocols at work. Collaboration: Promoting a collaborative approach to security, where individuals and teams work together to enhance overall security measures. By adopting a Security Mindset, individuals and organizations can better protect themselves, their data, and their assets from potential harm.

Security thinking can be correlated with various global indices measuring the level of security and security of countries and regions. Some indices that may correlate with safety mindsets include:

Global Peace Index: Measures the level of peace and security in countries and regions. Countries with a higher ranking on this index have less violence and conflict, which may reflect a more developed security mindset.

Global Cybersecurity Index: Assesses the readiness of countries to ensure cyber security. Countries with a higher ranking in this index may have a more advanced security mindset regarding cyber threats.

Global Terrorism Index: Assesses the risk of terrorism in different countries. Countries with lower levels of terrorism may have more sophisticated security thinking strategies.

Corruption Perceptions Index: Measures the level of corruption in countries. Countries with low levels of corruption tend to have more credible and effective security systems.

Human Development Index: Takes into account the level of education, health and standard of living of the population. A high level of the index may indicate a more conscious and educated population regarding security issues.

It is important to note that the correlation can be complex, as security mindsets can depend on many factors, including cultural, political, economic and educational aspects. However, these global indices may reflect the general level of security thinking in different countries and regions of the world.

Results. The Russian Federation's war against Ukraine has intensified existing challenges and created new threats for the entire world:

***Geopolitical and Geo-economic Threats*:** the global political landscape is constantly changing, leading to new tensions and conflicts. This can result in uncertainty and risks for companies operating in various regions as they must navigate shifting rules, trade policies, and security threats. The full-scale invasion of Ukraine by Russia in February 2022 created a geopolitical tsunami with significant economic, social, and political consequences for the European Union, particularly in its relations with Russia [7, 8, 9, 10, 11].

Terrorism is a constantly evolving threat that can take various forms. The Parliamentary Assembly of the Council of Europe adopted a resolution titled "Further Escalation of Aggression by the Russian Federation against Ukraine," in which the Russian regime was recognized as terrorist [7, 8, 9, 10, 11].

Cyber Threats: Due to increasing technological dependence, cybersecurity threats have become a significant problem. Since the start of Russia's full-scale invasion of Ukraine, the Ukrainian Computer Emergency Response Team (CERT-UA) has registered and investigated over 1,500 cyberattacks on Ukraine, the majority of which were attributed to Russia. The main targets of hackers include the governmental sector, information and energy infrastructure, as well as information-psychological operations and disinformation campaigns [12].

Media Threats: Propagandist social media, intimidation, disinformation campaigns, data leaks, and more. For instance, Russian occupants study information from social networks and intelligence data before launching missile strikes on Ukrainian territory [13].

The global rankings indicators of Ukraine deserve attention. The 2023 Global Peace Index (GPI), reveals the average level of global peacefulness deteriorated for the ninth consecutive year, with 84 countries recording an improvement and 79 a deterioration. This demonstrates that the deteriorations were larger than the improvements, as the post-COVID rises of civil unrest and political instability remain high while regional and global conflicts accelerate: Deaths from global conflict increased by 96% to 238,000, New data shows higher number of conflict deaths in Ethiopia than Ukraine, eclipsing the previous global peak during the Syrian war, 79 countries witnessed increased levels of conflict including Ethiopia, Myanmar, Ukraine, Israel, and South Africa, The global economic impact of violence increased by 17% or $1 trillion, to $17.5 trillion in 2022, equivalent to 13% of global GDP. Despite the conflict in Ukraine, 92 countries improved on military expenditure and 110 decreased their military personnel. Conflicts are becoming more internationalised with 91 countries now involved in some form of external conflict, up from 58 in 2008.

Impact of the War in Ukraine on Peacefulness: Ukraine recorded the largest deterioration, falling 14 places to 157th, The economic impact of violence has increased by 479% or $449 billion, equivalent to 64% of Ukraine's GDP, Despite the conflict, Russia's incarceration rate, violent demonstrations, terrorism impact and homicide rates have improved over the past year, with the homicide rate at its lowest since 2008, 65% of men in Ukraine aged 20 to 24 years have fled the country, or died in the conflict [14].

Assessment of Ukraine's economic freedom has been temporarily suspended due to Russia's ongoing invasion since February 24, 2022. A vibrant and resilient economy is an essential engine for Ukrainian freedom and independence. Ukraine's economic potential has long been suppressed by poor economic governance. Before the war, the foundations of economic freedom had been fragile and unevenly established across the country. Low rankings in the Index of Economic Freedom and other international studies have offered unambiguous indications of systemic shortcomings in the critical areas of transparency, efficiency, and openness that prevent the country's economic potential from being fully realized [15].

According to the updated "Human Flight and Brain Drain Index 2022" Ukraine ranks 81st in the world, being placed alongside Peru, Pakistan, Bolivia, and Angola. Our index score is 5.9. From 2007 to 2018, the brain drain index from Ukraine decreased from 7.5 to 4.8 (which is positive), but starting from 2019, the index has been steadily increasing. Human flight and brain drain index, 0 (low) - 10 (high), 2022 - Country rankings: the average for 2022 based on 41 countries was 3.66 index points.The highest value was in Albania: 8.3 index points and the lowest value was in Sweden: 0.6 index points. The indicator is available from 2007 to 2022. Below is a chart for all countries where data are available [16].

The trends of these ratings have been composed by the author. They demonstrate that the decline in the peacefulness rating is associated with a consistently critically low level of economic freedom, and a trend of increasing talent loss (Tabl. 1).

Tabl. 1. Dynamics of Ukraine's position in the rankings, 2014-2023

Ukraine	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Global Peace Index	2,2	2,48	2,72	2,92	2,79	2,75	2,72	2,52	2,69	3,04
Index of Economic Freedom	46,3	49,3	46,9	46,8	48,1	51,9	52,3	54,9	56,2	54,1
Human flight and brain drain index	5,7	5,4	5,5	5,4	5,2	4,9	5,2	5,5	5,8	5,9

Sources: developed by author

The Ukrainian context will change the emphasis of security thinking, taking into account the impact of a full-scale war waged by Russia against Ukraine.

Human-Centric Security: therefore, a person becomes the most important subject of creation, production and implementation of models of safety thinking, focused on safety, which is the basis of sustainability. This encourages us to move from a reactive security posture to a proactive one, allowing us to identify potential risks and vulnerabilities before they develop into serious incidents. In this context, the creation of a culture of safety thinking should be based on:

Continuous learning: Resilience to complexity requires us to learn throughout our lives. The ever-changing cyber threat landscape requires us to stay abreast of the latest developments in security trends, technologies and tactics. By continuously learning, engaging educational institutions and authoritative cybersecurity resources, we can gain the knowledge and tools we need to adapt to the ever-changing digital landscape.

Integration of multifaceted protective mechanisms: Security-oriented thinking requires a holistic approach to protection, multifaceted protection mechanisms.

Develop a culture of collaboration: The threat landscape is too large for any one person or organization to navigate alone. Cultivating a security-focused mindset encourages collaboration and sharing of information, expertise and stakeholders. By building strong partnerships, we expand our collective knowledge and incident response capabilities, creating a united front against threats.

A graphical interpretation of the components of the Ukrainian context of security thinking is presented in Fig. 1.

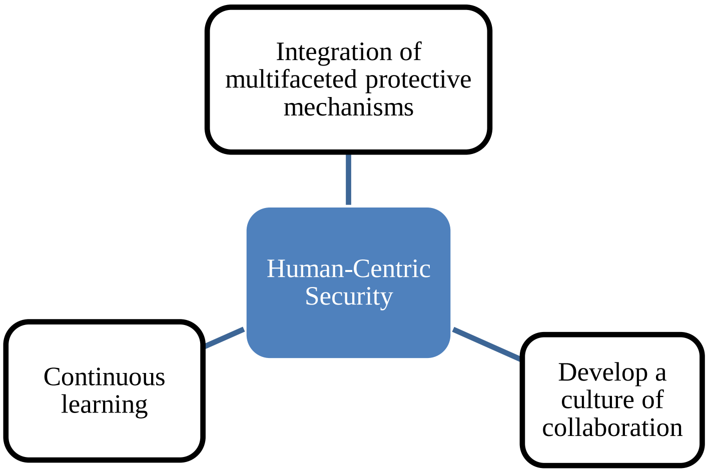
Integration of multifaceted protective mechanisms
Human-Centric Security
Continuous learning
Develop a culture of collaboration

Figure 1. The components of the Ukrainian context of security thinking
Sources: developed by author

Integrating Physical Security Measures: encompasses the integration of physical security measures. Physical access control, surveillance systems, and secure facility design are vital components of ensuring holistic protection. By recognizing the interdependence of digital and physical security, we construct a robust shield that guards against multifaceted threats.

Ensuring Compliance and Legal Security: in a world governed by regulations and legal requirements, adhering to compliance standards is paramount. A security-centric approach involves staying up-to-date with relevant laws and regulations, ensuring the protection of sensitive data, and safeguarding against potential legal liabilities. Upholding legal security bolsters our resilience against legal repercussions resulting from security breaches.

Promoting Social Engineering Awareness: as human behavior remains susceptible to manipulation, a comprehensive security-centric mindset addresses social engineering awareness. Training individuals to recognize and resist social engineering tactics, such as phishing and pretexting, reduces the risk of human error becoming an entry point for cyber attackers.

Protecting Data Privacy: the comprehensive security-centric approach includes safeguarding data privacy as a fundamental right. Implementing data protection measures, such as data encryption, access controls, and anonymization, demonstrates a commitment to maintaining the privacy of sensitive information and establishing trust with users and customers.

Embedding Security into Development Lifecycles: adopting a security-centric mindset at every stage of the software and system development lifecycle is crucial for building resilience from the ground up. Incorporating security by design principles ensures that security considerations are an inherent part of every development process, minimizing vulnerabilities and enhancing overall system security.

Proactive assessment of risks and response to incidents, potentially cascading risks and implications for economic, military, and societal security.

"Strategic offensive": accurate prediction of threats and prevention of their influence. Resilience to complexity means the ability to withstand threats.

Forming a security-centric mindset with consideration of Ukrainian context (Fig. 2) involves anticipating and adapting to the complex and constantly changing interplay of human behavior, processes, and technologies that characterize our interconnected world.

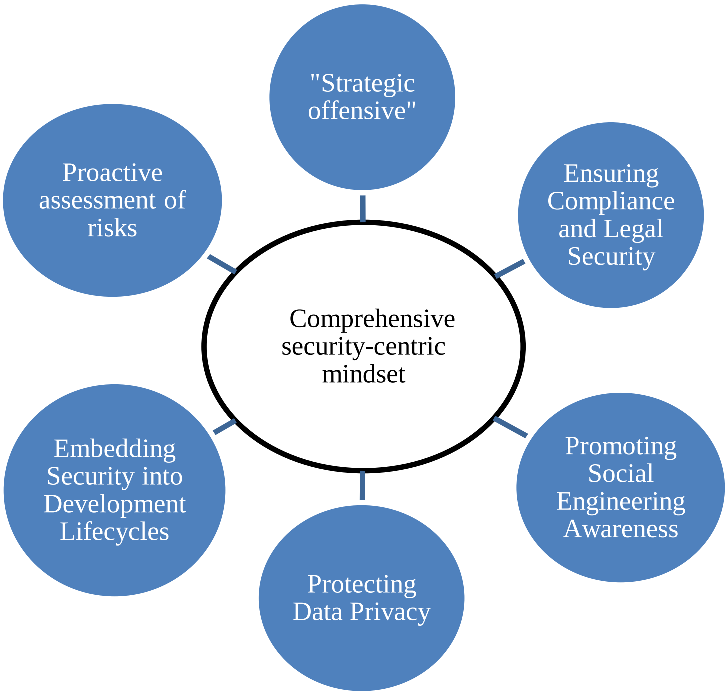
"Strategic offensive"
Proactive assessment of risks
Ensuring Compliance and Legal Security
Comprehensive security-centric mindset
Embedding Security into Development Lifecycles
Promoting Social Engineering Awareness
Protecting Data Privacy

Figure 2. A security-centric mindset with consideration of Ukrainian context
Sources: developed by author

Applying security thinking is a prerequisite for building resilience to complexity in the face of dynamic and unpredictable threats.

Discussion. Security thinking is related to the security culture. Attention is devoted to the security culture. The National Research Council of the National Academies of the USA published the study "Emergency Resilience: A National Imperative", which, in particular, outlines the vision of a resilient state. One of the important conclusions is that such a state, from individual citizens to the highest level of government, supports a culture of sustainability. As outlined in this study, a culture of resilience is based on the following key principles: individuals and communities recognize that they provide their own first line of defense against emergencies; the leadership of the state in the field of sustainability is realized through the adoption of political decisions, financing and corresponding activities of the parliament and all state authorities; at the state and regional levels, investments are made and efforts are made to increase the resilience of communities; information about risks and threats for specific objects is easily accessible, transparent and effectively disseminated, ways of managing risks and overcoming their consequences are discussed in communities; on the basis of information about risks and threats, resolutions and orders are adopted and implemented to protect critical functions; construction regulations and standards are adopted and strictly followed; much of disaster recovery is financed by private capital and insurance payments; the amount of insurance premiums depends on the level of risk, as well as compliance of objects (in particular, buildings) with established norms or modernization standards; to speed up the recovery process, community associations have emergency action plans to ensure continuity of governance, business, and service delivery, especially for the most vulnerable population groups; post-emergency recovery is significantly accelerated by sufficient capacity redundancy, timely upgrading and strengthening of infrastructure, taking into account regional interdependencies. Thus, the formation of a safety culture is both a prerequisite and a consequence of the formation of security thinking [17].

Conclusions. Developing a security mindset is not an end point, but a continuous journey. Using intellectual rigor and an innovative spirit, you can significantly influence the formation of a security ecosystem. The principles of resilience to complexity and a holistic approach to security, guided by a security-centric mindset, are becoming a dynamic force in protecting the security ecosystem. By integrating physical security, modernized legislation, social engineering, data privacy protection and psychological security, we can build a fortress against a wide range of threats. However, the unprecedented challenges associated with Russia's full-scale war against Ukraine have significantly complicated the architecture of modern security, creating a need for the development of a new paradigm of security thinking and practical tools for its application.

A security-oriented mindset is becoming a dynamic force in protecting the global ecosystem. Currently, a "fortress" is being created in Ukraine against a wide range of modern threats caused, above all, by Russia's aggression. Facing the challenges and complexities of modern security, we need to carry out scientific research on holistic and adaptive security-oriented thinking.

References:

1. *Disaster Resilience*: A National Imperative URL: https://www.nap.edu/download/13457

2. *Stephen M. Bellovin, Thinking Security*: Stoping Next Year's Hackers, Addison-Wesley Professional Computing ISBN: 978-0-13-427754-7 380 p.

3. *Buzan B., Waever O.* Security: A New Framework for Analysis. — Boulder: Lynne Rienner Publishers, 1998.

4. *UNDP. Human Development Report* 1994. Oxford : Oxford University Press, 1994. URL: http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostat s.pdf

5. *Held D., McGrew A.* The End of the Old Order? Globalization and the Prospects for World Order. Review of International Studies. 1998. Vol. 24. No. 4. Pp. 219– 245.

6. *Chandler D*. Resilience and human security: The post-interventionist paradigm. Security Dialogue. 2012. No. 43(3). Pp. 213–229.

7. *Reznikova O., Voytovsky K., Lepihov A*. Organization of the national resilience system at the regional and local levels : Analytical Report]. K. : NISS, 2021. 140 p

8. *Reznikova O.* (2022). Strategic analysis of the security environment of Ukraine / O.V. Kyiv: National Institute of Strategic Studies https://niss.gov.ua/news/statti/stratehichnyy-analiz-bezpekovoho-seredovyshcha-ukrayiny.
9. Frederick, B., Charap, S., Boston, S., Flanagan, S.J., Mazarr, M.J., Jennifer, D.P., Moroney, J., and Muller, C.P. (2022). Ways of Russian escalation against NATO from the war in Ukraine. RAND Corporation, https://doi.org/10.7249/PEA1971-1
10. Benjamin, J., Adrian, B. (2022). The coming storm: Ukraine's views on the escalation of modern warfare. CSIS Center for Strategic and International Studies. https://www.csis.org/analysis/coming-storm-insights-ukraine-about-escalation-modern-war
11. Sweiss, T., Bertolini, M. (2022). How wars end. Stopping the War: Perspectives on the Russian-Ukrainian War. The Hague: The Hague Center for Strategic Studies https://hcss.nl/wp-content/uploads/2022/05/How-Wars-End-HCSS-2022.pdf
12. https://ms.detector.media/kiberbezpeka/post/30938/2023-01-03-vid-pochatku-vtorgnennya-v-ukraini-zafiksuvaly-1500-kiberatak-sered-golovnykh-tsiley-informatsiyni-operatsii-ta-vkydy
13. https://nv.ua/ukr/ukraine/events/rf-vikoristovuye-socmerezhi-dlya-raketnih-udariv-po-ukrajini-novini-ukrajini-50291904.html
14. https://www.visionofhumanity.org/maps/#/
15. https://www.heritage.org/index/country/ukraine
16. https://www.theglobaleconomy.com/rankings/human_flight_brain_drain_index/Europe/
17. *Reznikova O. O.* National stability in the conditions of a changing security environment: monograph. – Kyiv: NISS, 2022. – 532 p.