UDC 343.33
DOI: 10.46493/2663-2675.34(1).2024.57

Stepan Dmytrenko*
PhD in Political Sciences, Assistant Professor
National Pedagogical Dragomanov University
02000, 9 Pirogova Str., Kyiv, Ukraine
https://orcid.org/0009-0005-4163-0468

Espionage counteraction as national security paradigm of 21st century

Abstract. The research relevance is determined by the advancement of technologies in contemporary society, which expand the possibilities and methods for committing espionage crimes. Accordingly, countering espionage in all its modern manifestations is an urgent task for the authorities and the legal system. The study aims to explore espionage, modern tactics, and strategies employed by global leaders to counter it, with a particular focus on the legal aspects. The primary approach utilized in this study is comparative legal analysis, which was used to analyse the approaches of states of several continents in countering espionage to protect national security. The formal legal method was also employed. The research involved a legal examination of the concept of "espionage" and explored various approaches adopted by states with differing economic statuses to combat contemporary espionage techniques. Additionally, a comparative assessment of national legal frameworks aimed at identifying new espionage methods, preventing criminal offences against national security, and mitigating the adverse effects of espionage on governmental, political, economic, and social domains was conducted. Primarily, the study holds theoretical significance, as it culminates in a comparative analysis of espionage countermeasures across states with varying economic capacities. These findings could potentially inform enhancements to espionage countermeasures within state systems, where such tools are obsolete and fail to address contemporary challenges effectively in the face of new technological ways of committing a criminal offence against national security by espionage

Keywords: cybercrime; spy; sovereignty; cyberspace; anti-spying measures; intelligence security protocols

Introduction

The policy of national security protection consists of several components. The national security policy is of foremost importance, as it sets the vector of activities for law enforcement agencies and sets priorities for the authorities to guarantee the safety and protection of both citizens and the nation. According to the definition provided by the UN Special Group on Security Sector Reform, this policy encompasses the perspectives of the government, and various institutions, and meets the requirements of the ultimate beneficiary – the citizen. The responsibility of authorities and law enforcement agencies is to prevent and combat crimes that pose a threat to national security. Crimes against national security are considered critical in terms of their level of public threat, since they encroach on information that holds state secrets, which directly endangers the constitutional order of the state, and its sovereignty, including territorial, economic, political, and independence of the state. Thus, the crimes described above threaten not one or several individuals, but the entire population of the state. The significance of national security has grown notably due to shifting dynamics on the global stage and the emergence of an "open state" trend. Yet, in the 21st century, the rapid advancements in information technology underscore the criticality of safeguarding state secrets from external threats. This is particularly crucial as the outcomes of intellectual endeavours in information technology can be exploited for illicit purposes, which expands the ways of espionage.

Z. Bederna & T. Szadeczky (2020) addressed the expansion of espionage methods using information space, focusing on the insecurity of the internet due to botnets used to engage in cyber espionage. B.R. Early and E. Gartzke (2021) contributed to the exploration of this subject, discussing the impact not only of information technologies on espionage but also the space technologies, namely satellite espionage. The authors assert that reconnaissance satellites fundamentally transformed the espionage-sourced intelligence, to the extent of preventing major conflicts between many states up to a certain point. This prompts a study of whether limiting the right to privacy is warranted to combat espionage and uphold national security. D.A. Alba Useche (2021) researched this

Received: 06.11.2023, Revised: 05.02.2024, Accepted: 29.02.2024

Suggested Citation:

Dmytrenko, D. (2024). Espionage counteraction as national security paradigm of 21st century. *Foreign Affairs*, 34(1), 57-62. doi: 10.46493/2663-2675.34(1).2024.57.

*Corresponding author

area, concluding that the issue of countering espionage was most relevant during the Cold War. D.A. Alba Useche addressed this issue on the examples of the USA and Russia, claiming the rapid development of monitoring software, information analysis, and the use of cyberspace to protect against cyber espionage and proves the existence of transgressions of the citizens' rights to privacy in exchange for surveillance "for the sake of security". The importance of addressing espionage, particularly cyber espionage, extends beyond national boundaries and becomes prominent at the international level. As such, R. Buchan & I. Navarrete (2021) note the role of international law in regulating cyber espionage, emphasising that, because of its "invisibility", cyber espionage has a destabilising effect on international cooperation and the stability of the international economic order. Adding to this discourse, O.H. Maican (2019) explores the legal dimensions of economic espionage. O.H. Maican clarifies that economic espionage involves the unlawful acquisition of vital economic intelligence, encompassing trade secrets and intellectual property, across sectors such as technology, finance, and governmental policies. The unauthorized access to vital proprietary information results in economic losses for the affected parties.

N. Eftimiades (2019) provided a comprehensive analysis of Chinese espionage. As an analyst for the Defence Intelligence Agency, N. Eftimiades provides an in-depth analysis of the organization, tactics, and operations of intelligence services operating within the People's Republic of China. He addressed the Ministry of State Security, illustrating how it utilizes diplomats, commercial representatives, overseas Chinese communities, and students to collect intelligence. Notably, China dispatches around 40,000 students abroad annually, contributing to its intelligence-gathering efforts. N. Eftimiades also highlights the case of Larry Wu-Tai Chin, a former CIA employee convicted of espionage in 1986, to provide insights into Chinese espionage operations in the United States. While acknowledging the Ministry of State Security's persistent efforts to infiltrate and exploit political, academic, industrial, and technological institutions in Western countries, N. Eftimiades also highlights the bureaucratic hurdles and constraints imposed by the Chinese Communist Party on the Chinese intelligence apparatus. The complexity of bureaucracy, according to N. Eftimiades, is an issue with the effectiveness of Chinese intelligence operations, offering some reassurance amidst concerns regarding Chinese espionage.

Hence, the study aims to explore contemporary espionage techniques and counterstrategies employed in the modern world, compare approaches to combating espionage adopted by world leaders and offer recommendations for improving counter-espionage mechanisms in state systems where existing tools are outdated and insufficient.

Materials and Methlods

The primary approach employed in this study is the comparative legal method, which was used to address the approaches of different countries in countering espionage to safeguard national security. Additionally, the formal legal method is used to conduct a legal analysis of the term "espionage" and its manifestations. The research framework incorporates international legal treaties relevant to countering espionage, including the United Nations Convention against Transnational Organized Crime and its Protocols (United Nations Convention against..., 2003), as well as The Budapest Convention (ETS No. 185) and its Protocols (The Budapest Convention..., 2000). The study investigated the doctrine as basic interpretations of espionage and ways of its commission. National regulations are of immense importance in estimating the degree of the state's counteraction to espionage, mechanisms, and modern techniques, as well as methods of reducing detrimental effects of espionage on political, economic, social, and other processes. The national security policies of certain states were analysed for their compliance with international legal treaties. The study also used analytical and statistical resources in the sphere of counteracting crime against the national security of international organisations.

The study was conducted in three phases. In the initial stage, a legal analysis of the concept of espionage was performed, covering the scope and methods of commission. The approaches of various states to this criminal offence were considered. The statistics of committing crimes against national security by espionage were investigated. The study covered the criterion of differentiation of infringement upon the rights to privacy and personal inviolability and the validity of such restrictions of rights to ensure national security. The nature of the information constituting a state secret was determined, which is most frequently the object of encroachment. The goals of state espionage and ways of bringing the subjects of a criminal offence to justice were also addressed. The second phase of this study analysed the global threat of espionage, particularly exploring contemporary methods of perpetrating this criminal offence through information technology, cyberspace, botnets, and outer space. The evolution of espionage as a crime against national security in tandem with technological advancements was analysed. Furthermore, the study delved into strategies for countering espionage in the digital realm and tactics for identifying perpetrators of espionage crimes. The features of espionage in the 21st century were considered, including various types of espionage: state, economic, network, and mobile espionage. The third stage covered a comparative analysis of states of different economic development (the United States of America, England, Azerbaijan, Indonesia, China, and Turkey) in terms of national policy on countering espionage. An analysis of the national and legal policies of states concerning the detection of new espionage methods, combating criminal offences against national security, and implementing mechanisms to mitigate the negative repercussions of espionage across state, political, economic, and social domains was conducted. The correlation between a state's global standing and its level of control over national security was determined. Conclusions regarding the most effective strategies for countering espionage were drawn, aiming to enhance existing mechanisms within state systems that are outdated and inadequately equipped to address modern challenges posed by new technological methods of committing espionage offences against national security.

Results

Espionage, as a criminal act against national security, has a long global history. However, with technological advancements and the rise of terrorism, along with corresponding countermeasures, espionage has become increasingly intricate and has sparked numerous international disputes. International law differentiates between espionage during peacetime and wartime. During peacetime, the principle of the separation of national and international jurisdiction, as well as the principle of equality among states, is upheld. Thus, any form of interference, including espionage, that violates a state's national jurisdiction is deemed illegal. The principle of equality among states underscores non-interference in each other's internal affairs. Nevertheless, the evolving international legal framework recognizes certain justifiable instances of intervention, including espionage, such as UN Security Council-authorized interventions to ensure global peace and security, self-defence, interventions upon invitation, humanitarian interventions, and interventions aimed at safeguarding human rights (United Nations Convention against..., 2003).

During wartime, under specific conditions, espionage is acknowledged as a permissible military tactic. There is a pressing necessity to establish a universal document to formalize the regulations governing espionage and its contemporary manifestations, such as cyber espionage and privacy-breaching espionage. Espionage causes global concerns, thus the new treaty can outline instances of lawful and unlawful espionage. The most severe crimes against state sovereignty in both the Anglo-Saxon and Romano-German legal traditions are high treason and espionage, which significantly undermine national security and encroach upon the rights and liberties of the populace, including citizens, stateless individuals, and foreigners (The Budapest Convention, 2000). Espionage has been present throughout human history. However, with shifts in human behaviour, the ways of engaging in espionage also changed. Presently, in most states, espionage as an offence against national security is considered through an objective paradigm. Espionage involves the transfer or gathering of information classified as a state secret, to pass it on to a foreign state, organization, or their agents. Importantly, these actions are typically carried out by foreigners or stateless individuals. Objectively, espionage is not considered to be committed by a citizen of the state from which the information is being collected. Such actions committed by a citizen are considered high treason in many states.

Significantly, the objective aspect of espionage does not cover an exhaustive list of methods by which espionage can be perpetrated. Consequently, practical espionage evolves in line with advancements and developments in information technologies. In the contemporary era, espionage is more accessible and simpler to execute compared to previous centuries (Alba Useche, 2021).

Features of espionage in the 21st century. The advancement of information technology significantly increased espionage, as it has become more accessible to more states. Due to quantitative changes, qualitative changes also occurred since conventional espionage was less dangerous and did not require any deep-state operations (Maican, 2019). Considering these factors, cyber espionage challenges the international legal system, as it has unique features, which distinguish it from conventional espionage regulated by the international community (Early & Gartzke, 2021). At this juncture in the evolution of international law, entities governed by international law can invoke the principle of non-interference in a state's internal affairs, thereby seeking to limit the scope of cyber espionage facilitated by technology. Methods of cyber espionage are developing in parallel with the advent of new software. The most common methods are presented in Table 1.

Table 1. The most common methods of cyber espionage

Method	Description
Malicious spyware	Can be used and distributed over the entire Internet.
Stalkerware	Spies gain access to a website or computer using a special program.
Targeted attacks	Set of cybercrimes aimed at a particular organisation, which entail data leakage, access to the restricted protected, etc. This method of cyber espionage is the most effective.

Source: B.R. Early & E. Gartzke (2021)

Regarding information as the target of espionage, several types can be highlighted based on its content. State espionage typically focuses on acquiring information classified as a state secret or military secret, the disclosure of which directly harms the independence of the state and its sovereignty. Industrial espionage is committed to eliminating a competitor or obtaining information that is considered a trade secret and contains intellectual property rights. Economic espionage is essentially similar to industrial espionage, but the object of encroachment can be both a commercial organisation and the state (Maican, 2019). Network espionage is also considered quite common, being committed remotely via the Internet by collecting "*cookies*" that store user data. Cyber espionage poses new challenges to international law. The main regulation that governs cyber operations and cyber espionage is the Tallinn Manual, which is based on previously formulated provisions on espionage, but transposed to cyberspace (Schmitt, 2017). However, the Tallinn Manual cannot be regarded as perfect regarding the specific features of the field of committing offences by espionage. Thus, the international community needs to develop practices to regulate cyber espionage, and then develop an international legal treaty based on such practices, which would include the responsibility of states for cyber espionage or inaction in the fight against it.

Methods of combating espionage in public administration: an international aspect. Counterespionage methods are integral components of national security policies, shaped by several factors. These include

the stability of international relations with key global actors, the existence of adversaries in international relations, and the significance of information for the internal advancement of the state, which constitutes the volume of state secrets. Given these factors, different states may have their specific features of the national policy of countering espionage, however, the overarching goal of safeguarding the sovereignty of the state remains consistent and unifying. Therefore, Turkey endeavours to maintain a balance both in countering espionage and in navigating the complexities of the international political landscape. Being between two opposing approaches in managing cyberspace and having close military ties with the West in the field of security, Turkey's domestic policy is more similar to the Russia-China axis, which is described by increased control over information and increased efforts to establish "digital sovereignty" in the national cyberspace (Schmitt, 2017; Atwood, 2019).

China has been engaging its internal anti-espionage measures for a long time, as China remains a closed state and, in the policy of an "open" society, resorted to strict anti-espionage regimes at all social levels (Eftimiades, 2019). Notably, China raises espionage issues in the information field amidst the international disputes on increased espionage towards China. Thus, following the proceedings on the doubled-down espionage by the United States, China adopted a regulation that assumes that government and party bodies, public and social organisations, and representatives of large business activities are primarily responsible for preventing espionage activities within their structures (Iasiello, 2021). Thus, China introduces control at the primary stage of access to state secrets, thus preventing any spies among personnel. The government places great emphasis on the education of both civil servants and the population in the field of countering espionage, as it believes that spies are not narrowed down to individuals who have direct access to state secrets – any active Internet user can become a victim of espionage (Rosicki, 2021).

During the Second World War, Britain implemented the "Careless conversation costs lives" policy, while the USA had a similar campaign known as "Loose lips sink ships" (Kearns, 2022). These initiatives aimed to deter individuals from spreading rumours or truths that could undermine morale or create discord among different population groups. However, with the rise of the information society, such tactics have become less effective. The British Security Service MI5 classifies espionage as a persistent threat to the UK. In the last century, the object of espionage was usually information (state secrets) that concerned state organisations since the goal was to obtain political and military information. In the 21st century, the target of espionage is information (industrial secrets, commercial secrets) from commercial organisations for their valuable research and know-how. In the modern world, the main methods of intelligence gathering exercised by MI5 can be classified as follows: secret agent sources – an individual who collects and transmits information containing state secrets; direct surveillance (shadowing and/or surveillance of objects); interception of messages (eavesdropping on phone calls or reading electronic messages); electronic surveillance (installation of listening devices in the house, flat, or car of the surveillance object) (Peek, 2012; 2013).

Indonesia is an example of a country with a developed legal system in the context of combating cyber espionage. In 2008, this country enacted legislation addressing cybercrime at the national level, along with regulations on such cyber activities. This is outlined in the Information and Electronic Transactions Law (UU ITE). Article 31 defines the interception of electronic information/electronic documents that belong to another person as illegal. Exceptions are cases when wiretapping is allowed when it occurs during a trial and reveals the commission of a crime (Satria Unggul & Noviandy, 2019).

The opinion of some Polish scientists is of interest, as they propose introducing changes in national legislation that criminalises espionage in Poland. They elaborate on the identity of crimes such as espionage and cyber espionage (cyberterrorism) and do not consider the latter as an espionage method. As arguments, they cite the fact that these offences have different objects of encroachment. In the first case, it is stated (national) security, and in the second – information security (Rosicki, 2021).

Espionage in the realm of innovation is a major concern in the United States. Consequently, the FBI organizes training sessions and creates guidelines for commercial enterprises in Silicon Valley. China poses the most significant threat to the United States in this regard. According to a report from the American CSIS Centre, the United States has closed over 160 espionage cases involving China in the past two decades. Concurrently, American companies have initiated approximately 1 200 lawsuits for intellectual property theft against Chinese entities during the same period (Grubbs, 2019; Korniychuk, 2023). Thus, it is possible to conclude that world leaders also need to regulate cyberspace and counter cyber espionage at the level of international law but to strengthen national security, states themselves need to abandon espionage towards opposing states.

Discussion

When examining espionage as a criminal offence against national security, this study concludes that the objective aspect of espionage, as a crime against national security, does not provide a comprehensive list of methods by which espionage can be carried out. Thus, the factual embodiment of espionage in the real world may change due to information technology advances as a result of using such progress with malicious intent. In contemporary society, it is much easier to become a spy since the methods of espionage are more accessible than in the past centuries. Z. Bederna & T. Szadeczky (2020) confirm the expansion of espionage methods due to the information space, focusing on the insecurity of the internet infected by botnets used to engage in cyber espionage. The methods of espionage mustn't be limited to the scope of information technology capabilities.

The opinion of some Polish scientists is of interest – they propose introducing changes in national legislation that criminalises espionage in Poland. They elaborate on the identity of crimes such as espionage and cyber espionage (cyberterrorism) and do not consider the latter as an espionage method. As arguments, they cite the fact that these offences have differing objects of encroachment. In the first case, it pertains to (national) security, while in the second case, it concerns information security. However, in

this article, the author holds the opinion that cyber espionage is espionage committed using cyberspace and other information technologies, but the object of encroachment is still a state secret, i.e., national security. On this occasion, I.V. Diorditsa (2020) provides an interpretation of cyber espionage, delineating several inherent features. As such, cyber espionage is characterised by the following attributes: illegal acts involving covert tracking, collecting, stealing, and transferring of information. The transferred information typically constitutes a state secret and is relayed to an external nation, foreign entity, or their delegates, all within cyberspace. The primary subject of this crime is information containing a state secret. According to I.V. Diorditsa (2020), the object of cyber espionage encompasses external national security, including the preservation of sovereignty integrity (territorial, political, and economic aspects), the maintenance of inviolability and defence capability, and ensuring security in the digital realm, encompassing information and cybernetic space.

E.N. Grubbs (2019) addressed espionage in a new aspect, elaborating on academic espionage. As such, the writer concludes that academic espionage is not a recent issue, but rather one that the US Congress has been diligently addressing. Lawmakers, governmental bodies, and educational institutions are actively assessing whether existing security measures are adequate to safeguard the intellectual property of the United States. E.N. Grubbs believes that the protection of academic institutions in the United States requires more awareness of academic espionage, rather than added security measures. The quantitative and qualitative analysis of statistical data on espionage in the United States confirmed the hypothesis of E.N. Grubbs since more crimes are related to intellectual property rights. Presently, the most critical issue is espionage in the realm of innovation. This is the reason why the FBI conducts training meetings and develops instructions for commercial companies in Silicon Valley to protect copyright and patent rights, which may have industrial secrets. According to the CSIS Centre, American companies have filed about 1,200 intellectual property theft lawsuits against Chinese legal entities, which confirms the threat to the United States from China in the realm of espionage (Mazzocco, 2024).

The conclusion states that the international community needs to develop practices to regulate cyber espionage, and then develop an international legal treaty based on such practices, which would include the responsibility of states for cyber espionage or inaction in the fight against it (Korniychuk, 2023). The anonymity of the user poses challenges in identifying the individual responsible for the offence, as well as in distinguishing between a cyber spy and a cyber intelligence agent. In practice, it is exceedingly difficult to conclusively determine whether the illegal gathering of information occurred within enemy territory, which entails difficulties in qualifying such an act as cyber espionage. Therefore, it is worth defining the boundaries of "digital sovereignty", which is quite difficult to do due to the popularity of blockchain and VPN technologies.

The thesis that cyber espionage poses new challenges to international law was also confirmed by other scientists. The relevance of the issue of countering espionage, especially cyber espionage, extends beyond the national level and escalates at the international level. R. Buchan and I. Navarrete (2021) discussed the significance of international law in managing cyber espionage, highlighting the destabilizing impact of cyber espionage on international cooperation and the stability of the global economic framework due to its "invisible" nature. Similarly, M. Jalali (2021) echoes this statement, underscoring the pressing necessity for a universal document to formalize regulations governing espionage, including emerging forms, such as cyber espionage and espionage involving privacy violations. Given that espionage has evolved into a worldwide issue, such a new treaty could delineate instances of both lawful and unlawful espionage.

In addition, using the example of Turkey, T. Eldem (2020) elaborates on the need to define the boundaries of "digital sovereignty". A similar opinion is expressed by M.A. Mudryak (2020) in his research, claiming that the information space has become the main arena of international clashes, where different-vector national interests of states collide, accompanied by fierce international competition for the use of information warfare. The rapid spread of telecommunication networks, electronic resources, and electronic delivery of information requires the state to develop a strategy to safeguard the information security of private enterprises, which should include the purpose, objectives, and a set of basic measures for its practical implementation. It should be a qualitatively new policy that, through information support, would effectively protect all areas of the economic policy at the national level.

Exploring the necessity of limiting privacy rights to combat espionage and ensure national security is a compelling area of study. D.A. Alba Useche (2021) delves into this topic, particularly focusing on its relevance during the Cold War era. By analysing the cases of the USA and Russia, the author highlights the rapid advancements in surveillance technology, information analysis, and cyberspace utilization in countering cyber espionage. However, this progress has raised concerns regarding infringements on privacy rights in the name of security. Counterespionage methods are influenced by technological and intellectual advancements, as well as its diplomatic culture and practices. Nonetheless, there is a pressing need for global consensus and unified strategies to combat the digital realm of espionage, particularly cyber espionage.

Conclusions

Examination of the notion of espionage and its evolution throughout history concluded that espionage cannot be committed by a citizen of the state against which information is being collected. Such actions committed by a citizen are considered high treason in many states. Additionally, the study discovered that the objective side of espionage does not define an exhaustive list of methods and mechanisms by which espionage can be committed. This circumstance is influenced by the potential for technology advancements to be exploited for nefarious purposes, including being a field of activity or a tool for a spy. Thus, the modern world faces the problem of espionage becoming much more accessible than in the past centuries. In this situation, only preventive measures can serve as effective countering mechanisms. The prevalence of cyber espionage

poses new challenges to international law. The most global concern is the complexity of personal identification in the digital world. Thus, in the pursuit of ensuring privacy in a digital society, the global landscape has reached a stage where maintaining anonymity serves as an advantageous factor for perpetrating various crimes, including espionage. Consequently, law enforcement agencies face challenges in identifying individuals, establishing their culpability in criminal activities, and discerning between a cyber spy and a cyber intelligence agent. Therefore, there is a pressing need to establish a clear definition of the term "digital sovereignty", to determine its scope, methods of security, and responsibility for encroachment. Thus, the international community needs to develop practices to regulate cyber espionage, and then develop an international legal treaty based on such practices, which would include the responsibility of states for cyber espionage or inaction in the fight against it. The findings of this study could serve as valuable resources for enhancing espionage countermeasures within state systems that are currently outdated and ill-equipped to address modern challenges posed by new technological methods of committing espionage offences against national security.

Furthermore, this study has raised new questions that require resolution. There is a need to further research and refine the norms of international law on cyber espionage and propose technical solutions to effectively counter such activities.

Acknowledgements

None.

Conflict of Interest

None.

References

[1] Alba Useche, D.A. (2021). Espionage and Security Agencies: The United States and the Russian Federation. *Science and Air Power*. Retrieved from http://repositorio.crai-fac.com/handle/20.500.12963/191.
[2] Atwood, R. (2019). *Combatting Chinese cyber economic espionage on the global stage*. (Doctoral dissertation, Utica College, Utica, USA).
[3] Bederna, Z., & Szadeczky, T. (2020). Cyber espionage through Botnets. *Security Journal*, 33, 43-62. doi: 10.1057/s41284-019-00194-6.
[4] Buchan, R., & Navarrete, I. (2021). *Cyber espionage and international law*. In *Research handbook on international law and cyberspace.* London: Edward Elgar Publishing.
[5] Diorditsa, I.V. (2020). The concept and content of cyberespionage. *Scientific Works of the National University "Odesa Law Academy"*, 26, 49-55.
[6] Early, B.R., & Gartzke, E. (2021). Spying from space: Reconnaissance satellites and interstate disputes. *Journal of Conflict Resolution*, 65(9), 1551-1575. doi: 10.1177/0022002721995894.
[7] Eftimiades, N. (2019). On the question of Chinese espionage. *The Brown Journal of World Affairs*, 26, 125.
[8] Eldem, T. (2020). The governance of Turkey's cyberspace: Between cyber security and information security. *International Journal of Public Administration*, 43(5), 452-465. doi: 10.1080/01900692.2019.1680689.
[9] Grubbs, E.N. (2019). Academic espionage: Striking the balance between open and collaborative universities and protecting national security. *North Carolina Journal of Law & Technology*, 20(5), 235-265.
[10] Iasiello, E. (2021). China arctic cyber espionage. *The Cyber Defense Review*, 6(3), 121-128.
[11] Jalali, M. (2021). Espionage in modern international law and necessity of codification of global provisions. *Public Law Studies Quarterly*, 51(1), 343-368.doi: 10.22059/jplsq.2020.216097.1351.
[12] Kearns, O. (2022). Forget what you hear: Careless Talk, espionage and ways of listening in on the British secret state. *Review of International Studies*, 48(2), 301-325. doi: 10.1017/S0260210521000589.
[13] Korniychuk, O.O. (2023). Experience of leading countries in responding to threats to national security in the process of decentralisation of the public management and administration. *Scientific Perspectives*, 2(32), 96-107. doi: 10.52058/2708-7530-2023-2(32)-96-107.
[14] Maican, O.H. (2019). Legal aspects of economic espionage. *Society of Juridical and Administrative Sciences*, 8(2), 385-392.
[15] Mazzocco, I. (2024). Chinese state and private firms. *CSIS*. Retrieved from https://bigdatachina.csis.org/unpacking-linkages-between-the-chinese-state-and-private-firms/.
[16] Mudryak, M.A. (2020). Separate issues of legal provision of information security of the enterprise in competitive relations: Intelligence and industrial espionage. In *Scientific collection "InterConf": Global and regional aspects of sustainable development (pp. 136-143)*. Copenhagen, Kyiv: SPC InterConf.
[17] Peek, S. (2012). Scientific and technical intelligence in the service of the state interest: Historical aspect. *Journal of the Lviv University. International Relations Series*, 31, 128-133.
[18] Peek, S. (2013). Intelligence activity in the modern world and its priorities. *Journal of the Lviv University. Series International Relations*, 32, 70-76.
[19] Rosicki, R. (2021). State security as exemplified by the offense of espionage under Polish law. *Remigiusz Rosicki*, 3, 49-73. doi: 10.14746/ssp.2021.3.4.
[20] Satria Unggul, W.P., & Noviandy, P.E. (2019). Analysist of cyber espionage in international law and Indonesian law. *Humanities & Social Sciences Reviews*, 7(3), 38-44.
[21] Schmitt, N.M. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Gambridge: Cambridge University Press.
[22] The Budapest Convention and its Protocols. (2000, November). Retrieved from https://www.coe.int/en/web/cybercrime/the-budapest-convention.
[23] United Nations Convention against Transnational Organized Crime and the Protocols Thereto. (2003, November). Retrieved from https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.