ЮРИДИЧЕСКИЕ НАУКИ

Prav R.Yu
Graduate student of the Interregional Academy of Personnel Management

FOREIGN EXPERIENCE OF STATE INFORMATION SECURITY POLICY AND COUNTERACTING INFORMATION THREATS

Annotation. The article analyzes the experience of EU state policy in ensuring information security and countering information threats. The relevance of theoretical and practical approaches based on the experience of leading EU to ensure information security in Ukraine is determined. The study analyzes the forms and types of threats to national security in the information sphere. The main aspects of international and national legal regulation of information security are considered. The key aspects of ensuring the network and information security of the EU states, the experience of European states in the development of laws and regulations in the field of ensuring national and public security are analyzed. The main international doctrinal documents that regulate the provision of information security in the world as well as in Ukraine, the legislation on the rights and obligations of the use and dissemination of public and private information as an object of intellectual property are listed.

Keywords: information security of Ukraine, national information space; information threats; information and psychological influences; information expansion, information wars and operations; mechanisms for counteracting information threats; state information policy.

Formulation of the problem and its connection with actual tasks. In the context of modern global and regional information confrontations, destructive communicative influences, clashes of diverse national information interests, the spread of information expansion and aggression, the protection of the national information space and provision of information security are becoming priority strategic tasks of modern states in the global information relations system. The preservation of information sovereignty, the formation of an effective security system in the information sphere is also an urgent problem for Ukraine, which is often the object of external information expansion, manipulative propaganda technologies and destructive information intrusion [7, p. 29]. It is essential to ensure the information security of the state by borrowing from the positive experience of European countries and other foreign countries, since Ukraine has suffered from information wars in recent years and can counteract their spread and negative consequences at a weak level.

Analysis of recent publications on research issues. The following scientists have been studying the problems of ensuring information security of Ukraine in the context of the analysis of foreign experience: D. Vasylenko, L. Hnatyuk, V. Gusarov, U. Ilnitskaya, O. Kostenko, V. Maslak, R. Marutyan, Y. Nesteryak, V. Petryk, T. Tkachuk, and others. However, the researchers have not identified the positive aspects of foreign experience that can be adapted in the Ukrainian realities.

Formulation of goals (purposes) of the article. The purpose of the article is to study the experience of the European Union (hereinafter - EU) countries for Ukraine in implementing the state policy on information security and combating information and cyber threats.

Statement of the main material. In recent decades foreign policy issues have been given special attention in foreign countries. Starting from 1994, the priority direction of the state information policy of many world countries has become a course on building an information society and the development of national and global information structures [12, p. 59]. In 1994, A. Gore proposed a plan for the development of the Global Information Infrastructure and formulated its five fundamental principles: 1) encouraging private investment; 2) promoting competition; 3) creation of a movable regulatory structure to support the pace of technological and market development; 4) providing open access to the network of all providers; 5) creation of Generic Service and organization of general service [12, p. 59]. These principles have formed the basis for building a system of interaction and communication based on advanced information infrastructure at different levels of government in the world.

In majority of developed world countries the legislation of information policy and information security has been creating for decades [12, p.21].

Nowadays the main international doctrinal documents governing information security in the world and in Ukraine are: Okinawa Charter of the Global Information Society (development and effective functioning of electronic identification, electronic signature, cryptography and other means of security and authenticity of operations) from 22.07. 2000; The Convention on Cybercrime of the Council of Europe, 23.11.2001; General Assembly resolution on "Advancing information and communication in the context of international security" (A / RES / 64/25) of 2 December 2009 and "Creating a global cyber security culture and assessing national efforts to protect critical information infrastructures" (A / RES / 58/199) of 23 December 2003, "Strategy in the field of information and communication technologies (hereinafter - ICT)" (A / RES / 57/304) of 15 April 2003, "Combating the criminal use of information technologies" (A / RES / 56/121) of 19 December 2001 and so on. The basic ideas of these documents express the desire for a more secure, stable, open global information space [21].

This legislation largely considers and defines the rights and obligations of the use and dissemination of information. In this setting, information is regarded as

an object of intellectual property rights, even when it comes to the mass media.

The North Atlantic Treaty Organization (hereinafter referred to as "NATO") pursues an active policy on information security, including the standards for the protection of information set out in CM (2002) 49 "Security in the North Atlantic Treaty Organization (NATO)", NATO's official cyber security policy. , a strategic cyber security concept, formulated on the basis of the Lisbon Summit and refined by the Warsaw Summit, etc. [2, p. 129].

Besides, a separate policy on information security and countering information threats has been established in the countries of the European Union.

A significant factor affecting European security is the strengthening of the international order, which depends on an effective system of multilateral treaties. In this regard, the formation of a system of international security-focused institutions is of particular importance. In this case, the role of the United Nations, the World Trade Organization, international financial institutions and the International Criminal Court cannot be underestimated. The European National Security Strategy attaches particular importance to transatlantic cooperation (in the form of NATO membership), the activities of regional structures (OSCE, Council of Europe, ASEAN, etc.) [5, p. 18].

In 2001, a document entitled “Network and Information Security: A European Political Approach” was presented by the European Commission outlining the EU's current approach to information security [18, p. 105]. In general, the strategic document outlines key approaches to the formation and support of information security of EU countries, namely: disseminating and report of accessible information on all possible types of threats that may cause changes in information security; dissemination of information on security and features of using network devices, software, etc; provision of appropriate technological support for users, as well as assistance of the state for the development of information infrastructure; stimulating innovation, including in the state-level cyberattack sector; development of effective mechanisms and algorithms for counteracting cyber threats and neutralizing their consequences in the shortest possible time; ensuring broad cooperation with other countries to counteract and avoid information threats and software corruption.

In 2007, the European Commission presented a document entitled "Towards a Common Cybercrime Policy", which defines cybercrime as criminal offenses committed by means of electronic communications networks and information systems, or against such networks and systems, and includes: traditional forms of crime (fraud and forgery in electronic communications networks and information systems); publication of illegal content in electronic media; specific crimes in electronic networks (attacks on information systems, hacking, etc.) [19, p. 139].

In order to strengthen the EU's ability to provide network and information security, the European Network and Information Security Agency (ENISA) was established in 2004. Their main objectives were [11, p. 104]:

1) to gather information to analyze and report potential information risks to member-states;

2) to increase cooperation at all levels to share experience in network and information security;

3) to monitor the development of standards in the field of security of services and products and to familiarize them with the participating countries.

The basic thesis for the EU member states in the field of information openness of public authorities and information security is: “it is generally accepted that a democratic system can function most effectively only when the public is fully informed” [9].

At the same time, the Council of Europe “Recommendation on Access to Information held by Public Authorities” states that, in order to ensure adequate participation of everyone in public life, public access to information which is at the disposal of state bodies of all levels should be ensured with inevitable exceptions and limitations. Thus, European standards of information for public authorities provide for their maximum information-openness, with the exception of restrictions related to the confidentiality of restricted information. First of all, it concerns the security of personal data [14].

In order to manage new potential threats, the European Union develops appropriate action plans by adopting adequate information legislation, taking into account national and international experience in regulating information relations, as well as creating an appropriate institutional mechanism established by a common system of bodies (European Council, European Commission, The Directorate-General for Education etc.) and specially created (The Directorate-General for Information Society, EU Forum of Information Societies). In the context of the problem of becoming an information society, the problem of ensuring information security is highlighted as a mainstay of the European Community's security policy. The European Union's information security covers the following aspects: Internet security (“Safer Internet plus (2005-2008)”, “Safer Internet (1999-2005)”); network security (information systems attacks, combating cybercrime); protection of personal data [11, p. 114].

The main document regulating the right of EU citizens to protect personal data is Directive 95/46 / EC “On the protection of individuals with regard to the processing of personal data and the free circulation of such data” [4]. This document simultaneously declares the desire for the free movement of information between EU Member States and provides guarantees for the protection of fundamental rights of citizens including the protection of personal data and the protection from third parties. The Directive obliges each EU member state to adopt its own law on the protection of privacy, which is compatible with the 1980 OECD recommendations [4].

Another aspect that needs to be noticed is the problem of information wars and information terrorism, which is by far considered to be one of the most urgent and dangerous threats carried by the development of information technology. Although there are many commonalities between information

wars and information terrorism (because in both cases there is an unauthorized, unlawful interference with information processes), the difference lies primarily in the subject of these actions (state or criminal or terrorist groups), the issue of information terrorism has become more widely recognized internationally, while the issue of information wars and information weapons has often remained beyond the scope of discussion [9, p. 81].

Thus, in 1996, United Nations Resolution 51/210 "Measures to Eliminate International Terrorism" (p. 3 (c)) "invited countries to implement counter-terrorism measures, including by creating appropriate legislation; to draw attention to the risk of terrorists using electronic or wired communications to commit criminal acts and the need to find means agreed with national law to prevent such crime from developing appropriate cooperation" [17].

On the contrary, the legal problems of information warfare and the regulation of the use of information weapons have been the subject of scholarly debate in the field of open information for a long time. On the initiative of the Russian Federation, this problem was formally recognized at the international level when resolution 53/70 "Advances in Information and Telecommunications in the Context of International Security" was adopted at the 53rd session of the UN General Assembly on 4 January 1999 [6]. The resolution expressed concern that the latest information technology and telecommunication technologies could be used for purposes incompatible with the objectives of international stability and security and could adversely affect the security of states, noted the need to prevent the misuse or use of information resources or technologies in criminal or terrorist purposes, and in this regard, UN member states were called upon to facilitate multilateral consideration of existing and potential threats in the field of information security [9].

The specificity of information weapons is that the object of its use can be any of the three types of elements of the information sphere: "Means and communication lines - the material basis of the world information infrastructure (it includes not only the means, interconnected by various channels communication, but also all equipment for processing information); information in its pure form and its flows; the person himself." Thus, the use of information weapons covers: destructive effects on material objects of the information sphere; destruction, distortion or alteration of information; purposeful influence on the nervous system, psyche and consciousness of a person [9, p. 83].

A significant step in establishing the international legal framework for the protection of information security was the signing by the Council of Europe of the Convention on Cybercrime, which took place in Budapest on November 23, 2001. Ukraine ratified this Convention in 2005. [9, c, 83] A feature of this international law the act is that it establishes a system of rules on the types of infractions using information and telecommunication technologies that Country Parties of this Convention are required to implement in national law.

The use of international and foreign experience in the formation of national state-legal mechanism of information security will avoid the so popular process of "reinventing the wheel" in our country, since there are quite a lot of countries with higher level of informatization that have previously faced the problems that Ukraine are facing today. The most appropriate organizational and legal approaches to the problem are implemented by the laws of the United States of America, Canada, and the EU Member States. In this setting, it is a question of borrowing constructive experience and abandoning steps that have led to negative consequences in the information sphere [9].

Attention to the problems of guaranteeing information security of Ukraine is conditioned by anti-Ukrainian influences, which promote the ideas of separatism, violence, national enmity and are attempts to destroy the national identity of Ukraine, its interethnic harmony, encroaching on the constitutional order of Ukraine, territorial integrity of the state. The problem of guaranteeing information security of Ukraine is actualized under the conditions of war on the East, when information expansion, biased and tendency coverage of facts and phenomena takes place on the part of the Russian Federation, and technologies of Russian information-psychological operations are aimed at securing dominance in the Ukrainian (as well as in the global) information space and to retaining media supremacy [14].

The experience of European states in the development of regulations in the field of national and public security can be applied during the preparation of acts of the Cabinet of Ministers and ministries aimed at implementing the National Security Strategy, approved by Presidential Decree No 287/2015 of May 26, 2015. For the purposes of the foregoing, it is advisable to carry out optimization of the activities of law enforcement agencies in Ukraine, taking into account the positive experience of foreign countries in creating a public security system and current global trends in the development of such systems by: enhancing cooperation with the European Union and NATO; improvement of anti-terrorist activity, regime of protection of state secrets; the concentration of intellectual, financial and other resources in priority areas for national and public security; raising the level of budgetary and other types of resources for public security entities [5, p. 20].

In order to counteract the large-scale negative information-psychological influences, operations and wars, the priority directions of the state information policy and important steps by the authorities of Ukraine should be: 1) integration of Ukraine into the world and regional European information spaces; 2) integration into international information and telecommunication systems and organizations; 3) creating their own national model of information space and ensuring the development of the information society; 4) modernization of the whole system of information security of the state and formation and implementation of effective information policy; 5) improvement of information security legislation, coordination of national legislation with international standards and

effective legal regulation of information processes [7, p.30].

It is evident that the priority tasks in the field of public information security management for Ukraine should be: improvement of legislation to counteract information threats; elimination of duplication of powers between the authorities providing the formation and implementation of information security policy; enhancing the overall level of communication and interaction between the authorities as well as the authorities with the stakeholders; improving the effectiveness of the implementation of the state policy of counteraction to threats; intensification of international cooperation in counteracting information threats; intensification of formation of own information policy and control over mass media in television space and networks; strengthening the control of cyber attacks.

Conclusions and prospects for further research. According to the study results, it can be summarized that the issues of ensuring the information security of the individual, society, the state, their protection against various kinds of threats, both external and internal, now occupy one of the leading positions in the priorities of state policy and strategies for ensuring the national security of European countries, the focus of which is oriented on EU and NATO approved standards. For Ukraine, as a state that has been confronted with the problems of hybrid warfare, it is very important to implement an information security policy in its territories for the allocation of a separate region called temporarily occupied territories. It would be appropriate to apply Germany's experience in the transition to the principle of "active defense" in providing information security, since the information security of the state is a continuous process of activities of competent authorities aimed at preventing, counteracting threats in the information sphere, as well as applying active measures of information influence. In addition, innovative technologies and methods of countering Russian information aggression should be used more intensively and a quality information product should be constantly presented.

In-depth analysis of innovative methods of counteracting information threats used by foreign countries and the possibilities for their application in Ukraine may also be promising in terms of further research.

References:

1. Belyakov, K. (2004). Informatyzatsiia orhanizatsiino-pravovoi suspilnoi diialnosti [Law of Ukraine] Kyiv [in Ukrainian].

2. Vasilenko, D.P., & Maslak, V.I. (2012). Zakonodavstvo providnykh krain svitu v sferi zakhystu informatsii [Bulletin of the KNU named after Mikhail Ostrogradsky] Kremenchuk [in Ukrainian].

3. Gusarov, V. (2014). Kreml rozpochav novu informatsiinu operatsiiu proty Ukrainy [Ukrainian pravda] (n.d.). https://www.pravda.com.ua Retrieved from https://www.pravda.com.ua/news/2014/09/3/7036659/ [in Ukrainian].

4. Dyrektyva 95/46/IeS Yevropeiskoho Parlamentu i Rady «Pro zakhyst fizychnykh osib pry obrobtsi personal¬nykh danykh i pro vilne peremishchennia takykh danykh» vid 24 zhovtnia 1995 roku [Legislation of Ukraine] (n.d.). https://zakon.rada.gov.ua Retrieved from https://zakon.rada.gov.ua/laws /show/994_242 [in Ukrainian].

5. Dytiuk, V.Z. (2015). Osoblyvosti normatyvno-pravovoho rehuliuvannia zabezpechennia publichnoi bezpeky v krainakh Yevropeiskoho Soiuzu [Bulletin of Lviv Polytechnic National University. Law Sciences] Lviv : Lviv Polytechnic National University [in Ukrainian].

6. Dostyzhenyia v sfere ynformatyzatsyy y telekommunykatsyi v kontekste mezhdunarodnoi bezopasnosty: Rezoliutsyia HA OON № 53/70 // Orhanyzatsyia Objedynionnykh natsyi. [UNODA] (n.d.). https://www.un.org Retrieved from http://daccessddsny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf?OpenEleme e.g. [in Russian].

7. Ilnytska, U. (2016). Informatsiina bezpeka Ukrainy: suchasni vyklyky, zahrozy ta mekhanizmy protydii nehatyvnym informatsiino-psykholohichnym vplyvam [Humanitarian vision] Kyiv [in Ukrainian].

8. Konventsiia pro kiberzlochynnist: Rada Yevropy; Konventsiia, Mizhnarodnyi dokument vid 23.11.2001: [Legislation of Ukraine] (n.d.). https://zakon.rada.gov.ua Retrieved from https://zakon.rada.gov.ua/laws/ show/994_575 [in Ukrainian].

9. Kormych, B.A. (2011). Pravovi vazheli protydii informatsiinym zahrozam : mizhnarodnyi i vitchyznianyi dosvid [Actual problems of politics] Odesa : Feniks [in Ukrainian].

10. Kostenko, O.V. (2015). Yevropeiski standarty pravovoho rehuliuvannia obihu informatsii z obmezhenym dostupom u roboti orhaniv prokuratury [Scientific herald of Uzhgorod National University: series "Pravo".] Uzhorod [in Ukrainian].

11. Maksymenko, Yu.Ye. (2007). Teoretyko-pravovi zasady zabezpechennia informatsiinoi bezpeky Ukrainy [Organizational and economic foundations of directions choice of innovative development of industrial enterprises]. Candidate's thesis. Sumy: SumSU [in Ukrainian].

12. Malyk, Ya. (2012). Zabezpechennia informatsiinoi bezpeky Ukrainy v konteksti svitovoho dosvidu [Effectiveness of public administration] Lviv : LRIPA NAPA [in Ukrainian].

13. Nesteriak, Yu.V. (2013). Mizhnarodni kryterii informatsiinoi bezpeky derzhavy: teoretyko-metodolohichnyi analiz [Bulletin of the National Academy of Public Administration under the President of Ukraine] Kyiv : NAPA [in Ukrainian].

14. Pro dostup do informatsii, yaka znakhodytsia v rozporiadzhenni derzhavnykh orhaniv: Rekomendatsii Rady Yevropy. – № K.(81)19 [Center for Democracy and Rule of Law] (n.d.). https://cedem.org.ua Retrieved from

https://cedem.org.ua/library/rekomendatsiya-r-81-19-pro-dostup-do-informatsiyi-shho-znahodytsya-u-rozporyadzhenni-derzhavnyh-organiv/ [in Ukrainian].

15. Pro zakhody shchodo vdoskonalennia formuvannia ta realizatsii derzhavnoi polityky u sferi informatsiinoi bezpeky Ukrainy: Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 28 kvitnia 2014 r. [Legislation of Ukraine] (n.d.). https://zakon.rada.gov.ua Retrieved from http://www.zakon5.rada.gov.ua /laws/ show/n0004525-14 [in Ukrainian].

16. Razmietaieva, Yu.S. (2016). Pryvatnist v informatsiinomu suspilstvi: problemy pravovoho rozuminnia ta rehuliuvannia [Law] Kyiv [in Ukrainian].

17. Rezoliutsiia 51/210 Heneralnoi Asamblei OON «Deklaratsiia, shcho dopovniuie Deklaratsiiu pro zakhody shchodo likvidatsii mizhnarodnoho teroryzmu 1994 roku» [Legislation of Ukraine] (n.d.). https://zakon.rada.gov.ua Retrieved from https://zakon.rada.gov.ua/laws/show/995_370 [in Ukrainian].

18. Tkachuk, T.Yu. (2017). Zabezpechennia informatsiinoi bezpeky v krainakh tsentralnoi Yevropy [Legal scientific electronic journal] Zaporizhzhia [in Ukrainian].

19. Tkachuk, T.Yu. (2018). Informatsiina bezpeky u systemi natsionalnoi bezpeky derzhavy [Education and science in the field of national security: problems and development priorities] Ostrog :

20. Tkachuk, T.Yu. (2017). Suchasni zahrozy informatsiinii bezpetsi derzhavy: teoretyko-pravovyi analiz [Entrepreneurship, economy and law] Kyiv [in Ukrainian].

21. Khanin, I.H. (2015). Formuvannia mizhnarodnoi systemy informatsiinoi bezpeky: ekonomichni oriientyry dlia Ukrainy [Effective economy] (n.d.). http://www.economy.nayka.com.ua. Retrieved from http://www.economy.nayka.com.ua/?op=1&z=4457 [in Ukrainian].

Peliukh O.S.,
PhD in Law, doctoral student
National Academy of the Security Service of Ukraine
Artiukhova N.O.,
PhD in Law, doctoral student
National Academy of the Security Service of Ukraine

DEVELOPMENT OF COUNTERINTELLIGENCE METHODS USED BY THE STATE SECURITY BODIES ON THE TERRITORY OF UKRAINE: RETROSPECTIVE ANALYSIS

Abstract. In the paper, the retrospective analysis of counterintelligence methods' application is carried out. It is found that the methods of intelligence and counterintelligence activity have been used since the formation of separate Kyivan Rus principalities on the territory of Ukraine. It is suggested that counterintelligence, as well as its methods, has received significant theoretical and scientific substantiation only since the second half of the twentieth century. However the effective application of such methods dates back to the Middle Ages, whereas their classification has remained practically unchanged till nowadays. It is proved that counterintelligence methods and techniques are undergoing constant changes and are in the process of dynamic development caused by the improvement of foreign intelligence services. Based on the results of the research, it is substantiated that the scientific approaches to methods as categories of counterintelligence theory and practice should be reconsidered in the contemporary context.

Key words: *counterintelligence, intelligence, agent method, provocation method, covert examination of mail, covert surveillance, criminal analysis method, operational game, combination.*

Introduction. The most important conditions for safe existence, viability and sustainable development of the state and society are protection of national sovereignty, social security and ensuring effective operation of all the state bodies. In this context, the protection of national interests from real and potential threats, risks and challenges lies within the competence of the intelligence services, whose primary function is counterintelligence. It is well known that the tasks performed by counterintelligence penetrate into almost all spheres of public relations, and their successful fulfillment neutralizes existing threats, ensures the country's prestige and competitiveness on the global arena and strengthens its international positions. Thus, modern counterintelligence is aimed at timely detection, prevention and suppression of the encroachments of foreign special services towards the national interests in vital sectors of social relations, in particular, economic, political, information, cyber, environmental spheres, etc.

Taking into consideration the above-mentioned, it is extremely urgent to analyze the development of counterintelligence methods from ancient times till nowadays, since modern research studies should take into account both positive and negative historical experience and practical heritage of past generations.

The study of the genesis of counterintelligence methods proves that this theoretical, applied and scientific category appeared at the same time with the introduction of the term "counterintelligence". Moreover, the study of the historical aspect of counterintelligence methods is of great importance for further development of their theoretical, legal and organizational foundations. In our opinion, mastering the experience of the past is determined by the need to develop basic and applied research aimed at improving counterintelligence methods.