МІЖНАРОДНИЙ ДОСВІД

УДК 351.746:007:355.01(477)

Hrebeniuk M. – Ph.D in Law, Associate Professor, Head of the Interagency Scientific and Research Center on Problems of Combating Organized Crime under the National Security and Defense Council of Ukraine, Kyiv, Ukraine

Institutional Provision of the Cyberspace Militarization in the context of the of Hybrid Threats Spread: Contemporary European Experience

In the modern world, cyberspace remains a place where the number of special military operations and confrontations is constantly increasing every year. An important component of the national cyber security system of any country in the world remains the state-guaranteed cyber defense which means a set of political, economic, social, military, scientific, scientific and technical, information, organizational and legal and other activities carried out in cyberspace and aimed at ensuring the defense of the sovereignty and defense capability of the state, preventing armed aggression. Therefore, in this article the author emphasize that there is an urgent need to accelerate the improvement of national legislation in accordance with the present challenges and application potential of the Internet to meet the challenges of armed struggle, which involves the active reformation of management systems by the relevant security sector; ordering the regulatory field, which should ensure the integrity of state policy in this area; active explanatory work among the population regarding possible risks as a result of cyber-threats; increasing the number of relevant departments involved in cyber defense system; the development of their own samples of cyber weapons and conducting trial cybernetic attacks, strikes in cyberspace; strengthening control over national cyberspace.

Keywords: cybercrime; militarization; hybrid threats; security sector; defense reform; cyber defense.

Problem statement. With the entry into force of the Law of Ukraine «On National Security» [1], the odious and progressive political course of Ukraine – joining NATO and the EU, the resolve of progressive development and modernization of the security and defense sector, has been clearly declared. The law systemizes the transition of the defense and security sectors of our country to NATO principles and standards. Consequently, we can state that in Ukraine there are radical changes in the security and defense sector. Against this background, an important component of the state policy in the sphere of national security and defense is the priority – ensuring cyber security. Taking into account the abovementioned, the issue of guaranteeing security in cyberspace is in the focus of the meticulous attention of the state apparatus and appears in most of the recently approved fundamental normative legal acts (National Security Strategy of Ukraine, Cybersecurity Strategy of Ukraine, Concept of development of the security and defense sector of Ukraine).

Without exaggeration, it can be argued that in the modern world, cyberspace remains a place where the number of special military operations and confrontations that are being conducted is constantly increasing every year. In modern cyber-world they occur not in a smaller quantity than on land, in the sea, air or outer space. So in this context one of the essential components of the national cyber security system of any country of the world remains the state-guaranteed cyber defense – a set a set of political, economic, social, military, scientific, scientific and technical, informational, organizational, legal and other measures that are carried out in cyberspace and aimed at ensuring the defense of the sovereignty and defense of the state, the prevention of armed conflict and the prevention of armed aggression [2].

Most of the world's leading countries are actively modernizing their own security sectors in accordance with the modern challenges and using the potential of the Internet to solve the problems of armed struggle that involves an active reform of the management systems of the relevant security sector; streamlining regulatory framework, which should ensure the integrity of state policy in this area; active explanatory work among the population about possible risks due to the implementation of cyber threats; increase in the number of relevant units engaged in the cyber defense system; the development of their own samples of cyber weapons and conducting trial cybernetic attacks, strikes in cyberspace; strengthening control over national cyberspace etc [3, p. 185].

Thus, at the level of the states of the world, there is generally accepted position that the important and relevant role in the provision of cyber defense is assigned to the creation of cyberforces. So, not accidentally, according to the conceptual provisions of the Law of Ukraine «On the basic principles of ensuring cyber security of Ukraine» [2], the Cyber Security Strategy of Ukraine [3], one of the key components of the national cyber security system is the national defense agency – the Ministry of Defense of Ukraine, which within the framework of its competence and in accordance with its functionality, tasks are assigned to prepare the state to repel military aggression in cyberspace (cyber defense); implementation of military cooperation with NATO related to the cyberspace security and general protection from cyber threats; providing cyber protection of its own information infrastructure.

It should also be noted that according to the Presidential Decree as of June 6, 2016 No. 240/2016 «On the decision of the National Security and Defense Council of Ukraine» of May 20, 2016 [4], in our country the Strategic Defense Bulletin has been adopted at the

legislative level, which will serve as «a roadmap» for the defense reform with the definition of ways to implement it in accordance with NATO standards. While substantively summarizing this document, it can be stated that within the framework of the defense reform, it is envisaged to create in the structure of the Ministry of Defense of Ukraine a subdivision of cyberforces (milCERT), which will act at the strategic, operational and tactical levels, to establish interagency coordination on these issues in the interests of ensuring the defense capability of our state etc.

Given the hybrid threats that the aggressor state is dynamically spreading around the world, for Ukraine the urgent task of political and military nature remains the creation of an adequate and reliable cyber defense system that would correspond to the best practices of the member states of the European Union and NATO. It should be emphasized that during 2017, a long-lasting work on the creation and maintenance of the NATO-Ukraine Platform to study the experience of combating the hybrid war in Ukraine continued, with emphasis being placed on the need to improve the identification of hybrid threats, strengthening the cyber defense of critical infrastructure, and intensifying practical sectoral cooperation between Ukraine and NATO.

Militarization of cyberspace can be considered one of the most important areas of state policy in this area. Despite the declared desire of international organizations such as the United Nations and most major geopolitical actors to counteract its militarization, one can expect further development of offensive and defensive means of warfare in cyberspace, given their potential effectiveness, until the emergence of a new «arms race» [5, p. 241].

It is no accident that back in February 2018, at a meeting of the National Coordinating Center for Cyber Security, the NSDC Secretary, realizing the scale of Russian aggression, including in cyberspace, announced the acceleration of the creation of a cyber defense unit in Ukraine.

The annual National Program under the auspices of the Ukraine-NATO Commission for 2018, approved by the Decree of the President of Ukraine dated March 28, 2018, No. 89, regulates the issues of cyber Security and its ensuring (p. 4.4.) [6]. Thus, in particular, the priority tasks for the current year are as follows: continuation of interaction with NATO in the field of cyber Security by ensuring cooperation within the framework of the NATO Trust Fund for Cyber Security; acceleration of Convention on cybercrime implementation in the domestic legislation; intensifying the development of international cooperation and interaction with the

competent authorities of other states in the field of countering cyber threats; strengthening of cooperation of state, including law enforcement and special bodies with the private IT sector in the field of countering cyber threats; creation of a system of rapid response to computer emergency events for the protection of information and state information resources in cyberspace, etc.

Proceeding from the above, it can be stated that under the conditions of reforming the security and defense sector of Ukraine, the important task of the state remains to ensure the compatibility of the Armed Forces of Ukraine with the armed forces of the NATO member states, and in the long term – Ukraine's acquisition of membership in the Alliance. Therefore, the acceleration of the implementation of NATO standards in the domestic defense sphere, as well as institutional creation and acquisition of cyberforces remains relevant for Ukraine. In addition, the implementation of the course of European integration and the development of a political dialogue with NATO in the context of an adequate response to hybrid cyber threats actualizes the need to highlight the best practices of EU experience in the developed initiatives with the aim of strengthening the level of cyber defense using the capabilities of the military defense sector.

The issues of ensuring the security of cyberspace in the EU member states and NATO member countries have been touched in their writings by such domestic scientists as: V.U. Bogdanovych, I. Diorditsa, O. Dovgan, D. Dubov, O. Klymchuk, V. Petrov, Ye. Skulysh, V. Shelomentsev and others. However, coverage of the measures taken at the EU level to quickly and adequately respond to the hybrid threats that the Russian Federation is creating lately, a review of the latest NATO initiatives on the militarization of cyberspace on a scientific level, none of these authors did, which reinforces the relevance of the topic of this scientific article.

The task of the authors is to summarize the initiatives developed and introduced with the participation of the EU member states, NATO, especially with regard to the functioning of cyber defense units (cyberforces), which ensure and guarantee cyber defense as an important component of the collective security system. Taking into account the need to strengthen the state of the cyber defense, in order to adequately respond to the current hybrid threats in cyberspace, the EU and NATO recognized the problem of building effective and reliable cyber defense one of the key in the modern world. In this connection, measures are being initiated, developed and implemented to strengthen parity cooperation between them in the field of cyber security.

Over the past years, the North Atlantic Alliance and the EU countries have resorted to active efforts to create their own modern cyber-weapon models, improve the cyber-command system and take coordinating measures in this area. This activity tends to dynamic growth. In July 2016 at the NATO Summit in Warsaw, cyberspace was recognized as the same area of operations as other traditional military spheres, and in February 2017, an updated Cyber Security Plan and «roadmap» for mastering cyberspace as a new area of operations were approved. Thus, the evolution of the cyber defense system of the EU is taking place, and cyberspace is recognized as the fifth theater of military operations, providing for the creation of military management, which should deal with coordination, planning and implementation of cyber operations. In turn, on November 8, 2017, a NATO meeting took place at the level of Defense Ministers, at which an agreement was reached on the establishment of a Cyber Operations Center, which would solve a number of strategic tasks.

Firstly, the creation of this structure has contributed to the institutional provision of the cyber defense and will provide an opportunity to integrate it into the planning of NATO operations at all levels. Secondly, it gave the cyber the opportunity for each member state to participate fully in missions and operations under the auspices of NATO while preserving nationality.

On November 6, 2017, the Alliance announced the preparation of a special doctrine of cyber-operations, in the provisions of which the Alliance's withdrawal from passive protection and transition to a strategy of pro-active defense in cyberspace are proclaimed. At the same time, based on the principles of developed security, NATO adheres to the strategy of retaining aggression on the part of the Russian Federation and preventing the spread of hybrid threats, that is, the use of cyber capabilities of NATO can be a more proportional response to various challenges. What is more, NATO's activities always correspond to the norms of international law, and therefore actions in cyberspace should not be an exception.

Given the prospects for NATO, the next stage in the development of the cyber defense of the Alliance member states should be the building up of both human and technical potential. Today most of the NATO member states have their own cyber security strategies, and in some of them, cyber commands and relevant units have been created. However, it is unknown how far these strategies are harmonized. At the same time, those countries that make the main contribution to the Alliance's funding play a primary role. According to 2017 data, the United States, Great Britain, France and Germany, as a whole, cover $ 825 billion out of

$946 billion in NATO expenditures, i.e. 87 %, and have their own cyber-assets and cyber-command. This experience is adopted by other member countries of the Alliance.

For example, Latvia formed the «MilCERT» group under the Ministry of Defense back in 2016. According to the order of the Minister of Defense of Latvia, «MilCERT» is operationally subordinated to the State Secretary of the Ministry of Defense. The strategic objective of this division is to continuously monitor cyberspace and information and communication networks in the Ministry of Defense of that country; identification, response, elimination of cyber incidents and their consequences in the field of defense. The MilCERT military command of Latvia is also an active participant in cyber training, whose representatives, starting from 2015, are constantly taking part in trainings conducted under the aegis of NATO «Cyber Coalition». This unit also carries out close cooperation in the field of cyber security with the civil emergency response team in the cyberspace «CERT.lv».

Since the hybrid war is part of the military doctrine of the Russian Federation, while responding to external threats, Germany, as a NATO member in April 2017, created the Cyber and Information Domain Service Headquarters (CIR) with a staff of 260 employees. Functional tasks of the cyber defense of Germany were to ensure the security of the information systems of the defense department, to protect the regular work of the critical information infrastructure of the armed forces. Thus, in 2017, the structure of German Armed Forces finally formed the cyber forces and taken into a separate type – along with land, air and sea forces, however until 2017 to ensure cyber defense in the country corresponded to the Ministry of Internal Affairs.

In July 2017, the number of members of the military cyber team increased to 13,500. It is expected that the peak of efficiency in Germany will take place in 2021, when the state of cyberforces will reach a total of 14,500 people, including 1,500 civilians. In Germany, cyber-units are a separate structure of the Bundeswehr and have quite a wide range of functions: in addition to conducting cyber operations, they are engaged in the protection of official and operational information, providing cyber security, taking electronic warfare measures, conducting military intelligence in cyberspace and etc.

In 2018, German Chancellor Angela Merkel announced a strategic course of national cyber security – accelerating the acquisition of cyberforces and their proper financial provision in accordance with NATO's objectives and national defense concepts. At the same time, taking into account such accents, it was determined the need to increase the amount of military expenditures

of the country in the coming years in order to strengthen cyber security measures. It is no coincidence that the German Defense Minister insists on increasing the financing of the armed forces by an additional EUR 12 billion over three years: in 2019, the Head of the German Defense Ministry proposes to increase financing by three billion euros, in 2020 – by four, and another five billion to allocate for 2021. In 2017, the country's defense expenditures amounted to 37 billion euros, or 1.2 % of GDP, although NATO requires member states to spend at least 2 % of GDP on defense.

The UK began to form its cyber forces as early as 2013 in accordance with the basic provisions of the United Kingdom's Cyber Security Strategy, for which the Joint Forces Cyber Group was established to plan and coordinate the conduct of special cyberoperations. It consists of united cyber units located in the UK Government Communications Headquarters (GCHQ), the Ministry of Defense, as well as cyber reserves and information service. In 2016, the United Kingdom made additional efforts to strengthen the protection of cyberspace by creating the National Cyber Security Centre.

France's priorities in cyberspace were defined in the White Paper of 2008, which refers to the need to develop combat capability in cyberspace. The updated White Paper 2013 repeated these ideas, confirming the need for comprehensive cyber defense capabilities. The French operational cyber command was created in December 2016, and according to the plan it carries out both counteractive and preventive and defensive operations. At the same time, generalization of France's strategic documents on the provision of cyber defense gives grounds to argue that they are somewhat different from the approach advocated by NATO. Unlike Germany's comprehensive approach and the combination of cyber operations with electronic intelligence, as envisaged in the United States and Great Britain, France has created a fairly compact, highly specialized structure of the highest strategic level. It is expected that until 2019, the cyber command will employ 2,600 cyber security professionals, while the financial costs of ensuring the operation of the new structure will amount to 2.1 billion euros over five years.

Poland was one of the EU countries against which large-scale cybernetic wars were waged by Russian hackers. Poland realized the danger of cyber threats after large-scale cyber attacks in 2012, as a result of which the work of government websites was paralyzed, and a wave of mass protests that began on the streets swept through the Internet via massive DOS attacks. In order to respond adequately to the cyber-threats that the aggressor country is constantly spreading, Poland was forced to implement a consistent state policy in the field of

cyber security, the main concepts of which were: adoption of legislative amendments that will provide an opportunity to introduce a state of emergency in the country in the event of massive attacks in the virtual space; development of a new Cyber Security Strategy; formation of cyberforces. Recognizing the responsibility, given the important role on the eastern flank of NATO, Poland, in order to combat Russian hackers in 2018, also formed an appropriate unit with a total of 1,000 troops, for which the Ministry of Defense of this country allocated more than 2 billion zlotys (more than 465 million euros). So, the NATO member countries, realizing the danger of cyber threats and chaos, the scenario of which the aggressor state tries to implement in the EU countries, are making important steps towards the creation of national military teams in cyberwar format. Thus, the creation of a reliable cyber defense in the territory of NATO is precisely the creation of cyberforces and cyber command, which will operate at the operational, strategic and tactical levels.

In parallel, NATO is building up its cyber-potential in other areas as well. Thus, cooperation with non-members of the Alliance is intensified; in particular Jens Stoltenberg visited Japan in October 2017 for this purpose. As part of the arrangements, the NATO Centre for Cyber Security, which is located in Estonia, will send Japanese experts and specialists to participate in comprehensive studies on cyber security. Also in the focus of attention of NATO and Japan are issues of active participation of the Japanese side in NATO exercises on cyber security. In 2018, it is planned to review the main directions of Japan's national defense program, and within the framework of this process, the Ministry of Defense plans to establish a Command Centre for the management of operations in cyberspace, which will interact with NATO and relevant structures of the United States. At the same time, the number of Japanese cyber security units will increase to 1,000 people. So, NATO and Japan, on a parity basis, jointly build military capabilities in cyberspace as allies.

Cooperation between Europe and NATO is developing on the basis of the general Declaration signed in July 2016, in the provisions of which cyber security and cyber defense are defined among the priorities. In December 2016, a list of 42 events was presented in seven directions defined in the Declaration, and on December 5, 2017, this list was supplemented by 34 new measures. On December 8, 2017, senior EU officials met with their counterparts at NATO Headquarters. At this meeting, they discussed both current and prospective activities, a new format for cooperation in the field of cyber defense and agreed that in order to strengthen the capabilities

of NATO and European defense cooperation, it is expedient to create a common European army.

On December 11, 2017, the Council of the European Union approved the creation of a new defense program (PESCO), which was joined by 25 EU countries. PESCO (Permanent Structured Cooperation) is an institutional permanent cooperation in the field of general security and defense in the EU. In particular, the following member countries have voluntarily joined the program: Austria, Belgium, Bulgaria, Czech Republic, Croatia, Cyprus, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Ireland, Latvia, Lithuania, Luxembourg, the Netherlands, Poland, Portugal, Romania, Slovenia, Slovakia, Spain and Sweden. This program does not include Great Britain, Denmark, and Malta.

Given this program, PESCO is an initiative and constructive platform for building defense cooperation, which aims to increase the operational readiness and unification of the national European armed forces. In addition, it was decided at the EU level to accelerate work on the gradual formation of the European Defense Fund, and therefore it was determined that the European Defense Industrial Development Program should be adopted in 2018, which would allow full-format financing of the first PESCO projects. According to the EU position, the PESCO program will not compete with NATO, which includes 22 EU member states, and it is expected that PESCO will complement and improve the defensive capabilities created on the basis of the Alliance.

NATO continues to fulfill its obligations to monitor cyber threats, organize cyber defense of member countries, and Europeans, within the framework of the newly established structure, have found ways to finance cyber defense, as PESCO will play an important role not only in strengthening defense, but also in developing investment partnership. In this regard, EU High Representative Federica Mogherini said that the EU offers a platform for joint investment and projects that will enable them to overcome fragmentation that characterizes the current state of the defense industry in Europe.

In March 2018, NATO member states agreed on a «road map» for the implementation of the European program (PESCO). According to its provisions, by June 2018 EU countries should develop the principles of strategic development and determine the general procedure for the implementation of this program and its management within the framework of joint defense projects. The EU Council also identified 17 priority projects in three main areas: training and professional development of military personnel; creation of joint systems for command, control and support of land, air, sea

and cybernetic operations, strengthening of military and technical cooperation and armament.

At the same time, taking into account the geopolitical position of the EU countries that have a common border with the aggressor state, the actualization of threatening trends in cyberspace directly related to the aggressive foreign policy of the Russian Federation, numerous hacker attacks, constant attempts to disrupt the regular mode of operation of critical information infrastructure in the EU countries and NATO, causing significant harm in such key industries as banking, IT, energy and transport infrastructure, in particular Baltic States, in 2018 Lithuania initiated the need for consolidation of efforts at EU level to strengthen cyber defense in the NATO format, an adequate response to cyber incidents and external cyber attacks.

For the first time in the modern history of the European Union on June 25, 2018, at the initiative of Lithuania, a Memorandum of Intent on the creation of the so-called «European Intervention Initiative» was signed with the participation of nine EU member states, which was announced at the initiative of Lithuania to implement a general political decision to strengthen the state of ensuring cyber security in the EU territory in Luxembourg the creation of cybernetic rapid reaction forces. The Defense Ministers of such countries as Lithuania, Estonia, Croatia, Holland and Romania addressed the memorandum. It is expected that France, Spain, Poland and Finland will join these initiatives before the end of 2018, and four more countries – Belgium, Greece, Slovenia and Germany will join the project as observers. A new European military project is aimed at conducting joint exercises and exchanging information between the General Staff of the Armed Forces, including between military cyber teams. As part of the agreements, cybernetic teams are united-the so-called «milCERT» will assist the EU member states in case of large-scale computer attacks and cyber incidence, help identify cases of encroachment on the military critical information infrastructure and prevent such cases within the Euro-space. The format of the «European Intervention Initiative» assumes the rapid response of the joint units of the EU cyber security to the current challenges and threats in cyberspace, with the rotation of cyberforces from each EU state scheduled every six months.

Such initiatives force EU policies to make proper financial provision for cyber security, including the allocation of funds under the EU budgetary defense programs to purchase all modern equipment and secure licensed software. The logic of the functioning of the joint cybernetic rapid reaction teams implies the involvement of

representatives of the emergency response group in cyberspace «milCERT» from each EU member state.

On the eve of the meeting of the Heads of Allies, on July 10, 2018, the EU and NATO signed a joint declaration on cooperation. This document foresees strengthening of EU-NATO cooperation in such spheres as military mobility, joint preparation for cyber attacks and counteraction to hybrid threats; the fight against terrorism and illegal migration, etc. [8].

Obviously, for Ukraine the issue of creating cyberforces is extremely necessary. Due to the fact that cyber threats have become an element of modern hybrid war, cyberforces should be created in the structure of the Armed Forces of Ukraine taking into account the positive experience of Lithuania and with the help of NATO. In February 2018, the Cyber Threat Response Centre under the State Service of Special Communication and Information Protection began operating in Ukraine, which will respond to cyber incidents, coordinate the work of cyber defense units of various law enforcement agencies, and carry out cyber attack prevention.

However, the actualization of the acceleration of the creation of cyberforces in Ukraine is directly related to threats and challenges on the part of the Russian Federation, where the units of information operations have already been set up to carry out military doctrine in the structure of the Armed Forces of the Russian Federation, which provide centralized cyber war operations, ensure the management of military computer networks, military command and control systems and their protection, are capable of infecting the critical infrastructure of other states, conducting special information operations, cyber attacks and, primarily, against Ukraine.

Conclusions. The continuous militarization of cyberspace, military aggression by the Russian Federation, including in cyberspace, require the adoption of adequate system-based response measures. In particular, the threat of using the domestic segment of cyberspace by the Russian Federation is not excluded in order to negatively affect the Ukrainian elections in 2019. In modern conditions, at the level of the political leadership of the state, the issue of the creation of cyberforces in the structure of the Armed Forces of Ukraine is being studied. Thus, in Ukraine, within the framework of state strategic planning and implementation of legislative initiatives in the sphere of development of the security and defense sector, it is expedient to speed up the formation of a new division of cyberforces in order to ensure the increased combat readiness of the country to conduct both local and large-scale wars and confront hostile special information operations.

The creation of the «milCERT» National military unit should be an important step towards the development of modern capabilities of a defensive nature and contribute to the effective fulfillment of military tasks in any conditions. Undoubtedly, this new unit of the Armed Forces of Ukraine shall comply with all NATO standards, including in the field of electronic communications, data protection, information security and cyber defense of critical information infrastructure for defense purposes. It is also believed that a promising accession to the «European Intervention Initiative» under conditions of an observer should be a useful experience for Ukraine.

REFERENCES

1. Zakon Ukrainy "Pro natsionalnu bezpeku": vid 21 chervnia 2018 r. No. 2469 [Law of Ukraine "On National Security" dated June 21, 2018, No. 2469]. (n.d.). *zakon3.rada.gov.ua.* Retrieved from http://zakon3.rada.gov.ua/laws/main/2469-19 [in Ukrainian].

2. Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy": vid 5 zhovt. 2017 r. No. 2163 [Law of Ukraine "On the Basic Principles of Cyber Security Protection of Ukraine" from October 5, 2017, No. 2163]. *Vidomosti Verkhovnoi Rady Ukrainy*, *45,* 403 [in Ukrainian].

3. Kosohov, O.M. (2015). Suchasna polityka bezpeky kiberprostoru v umovakh yoho militaryzatsii [Modern security policy of cyberspace in the conditions of its militarization] *Scientific Journal "Modern information technologies in the field of security and defens", 3,* 181-186 [in Ukrainian].

4. Nakaz Prezydenta Ukrainy "Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy": vid 27 sich. 2016 r. No. 96/2016. "Pro Stratehiiu kiberbezpeky Ukrainy": vid 15 berez. 2016 r. No. 96/2016 [Order of the President of Ukraine "On the decision of the Council of National Security and Defense of Ukraine" from January 27, 2016 "On the Strategy of Cybersecurity of Ukraine": Decree of the President of Ukraine" from March 15, 2016, No. 96/2016]. *Ofitsiinyi visnyk Ukrainy, 96/2016* [in Ukrainian].

5. Chetveryk, H.H. (2012). Napriamky realizatsii derzhavnoi polityky u sferi kibernetychnoi bezpeky [Directions for the implementation of state policy in the field of cyber security]. *Buleten Dnipropetrovskohgo Universiteta, Bulletin of Dnipropetrovsk University, 22,* 240-245 [in Ukrainian].

6. Nakaz Prezydenta Ukrainy "Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy": vid 20 trav. 2016 r. No. 240/2016: "Pro Stratehichnyi oboronnyi biuleten Ukrainy": vid 6 cherv. 2016 r. [Decree of the President of Ukraine "On the decision of the National Security and Defense Council of Ukraine" from May 20, 2016, No. 240/2016, "On the Strategic Defense Bulletin of Ukraine"] [in Ukrainian].

7. Nakaz Prezydenta Ukrainy "Pro zatverdzhennia Richnoi natsionalnoi prohramy pid ehidoiu Komisii Ukraina-NATO na 2018 rik": vid 28 trav. 2018 r. No. 89 [Decree of the President of Ukraine "On Approval of the Annual National Program under the auspices of the Ukraine-NATO Commission for 2018" from March 28, 2018, No. 89]. (n.d.). *www.president.gov.ua.* Retrieved from http://www.president.gov.ua/documents/892018-23882 [in Ukrainian].

8. NATO and EU leaders sign joint declaration. Retrieved from https://www.nato.int/cps/en/natohq/news_156759.html.

Стаття надійшла до редколегії 22.06.2018

Гребенюк М. В. – кандидат юридичних наук, доцент, голова Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України, м. Київ

Інституційне забезпечення мілітаризації кіберпростору в умовах поширення гібридних загроз: сучасний європейський досвід

У сучасному світі щороку постійно збільшується кількість проведених спеціальних військових операцій і протистоянь у кіберпросторі. Важливою складовою національної системи кібербезпеки будь-якої країни є гарантована державою кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, організаційно-правових та інших заходів, яких уживають у кіберпросторі, що спрямовані на забезпечення захисту суверенітету й обороноздатності держави, запобігання збройній агресії. Нагальною є потреба прискорення процесу вдосконалення вітчизняного законодавства відповідно до викликів сучасності та застосування потенціалу мережі Інтернет для виконання завдань збройної боротьби, що передбачає активне реформування систем управління відповідним сектором безпеки; упорядкування нормативного поля, що має забезпечити цілісність державної політики в цій сфері; активну роз'яснювальну роботу серед населення щодо можливих ризиків унаслідок реалізації кіберзагроз; збільшення чисельності відповідних підрозділів, зайнятих у системі кіберзахисту; розроблення власних зразків кіберзброї та проведення пробних кібернетичних атак, ударів у кіберпросторі; посилення контролю за національним кіберпростором.

Ключові слова: кіберпростір; мілітаризація; гібридні загрози; сектор безпеки; оборонне реформування; кіберзахист.