UDC 342.951:351.741

K. V. SOLNTSEVA,
Candidate of Legal Sciences, Associate Professor
of the Department of Administrative Law and
Administrative Activities Yaroslav Mudryi
National Law University

POLICE AS THE SUBJECT PROVIDING CYBERSECURITY

The article is devoted to some questions researching state policy in the cyber sphere and cybercrime legislation of some foreign countries, problems of administrative and legal regulation of policing in Ukraine, the improvement of the current Ukrainian legislation.

Researches in the sphere of cyber policing have got a special actuality in Ukraine recently, because the President of Ukraine has signed an order to enforce the Ukrainian National Security and Defense Council's resolution dated January 27, 2016, «On the Cyber Security Strategy of Ukraine», the one and only legislative act, which regulates the activities of the law enforcement bodies in this sphere. It creates conditions for safe operation of cyber space and its use in the interests of people, society and the government. Studying and using gained successful experience of the foreign countries is essential especially in order to improve the activities of the Ukrainian police.

Keywords: police, cyberpolice activities, cybercrime legislation, cyber security strategy.

Problem setting. The consequence of global informatization, which manages the existence and activities of countries of the world community nowadays, is the formation of global cyberspace. During this process the convergence of computer technologies is taking place, new methods and means of influencing the information infrastructure are being created, new resources are being generated and their main task is to protect state electronic informational sources and the infrastructure. One realizes that the network of computer hackers and financial fraudsters span the whole world, the infrastructures of the states are exposed of systematic and unprecedented complex cyber-attacks of unknown authorship, and attackers in different ways are trying to escape the justice and remain unpunished. However, having become aware of the growing imminence, which threatens to any country in the cyberspace, it is important for the governments to develop policies and strategies to implement programs running on cybersecurity, defining priorities and being guided by the principles, legal framework and international agreements. Cyber security is a strategic issue of the national importance that affects all sectors of the society. Prudent public policy of the cybersecurity serves as an absolute means of strengthening the security and reliability of informational systems of any state.

The object of this study is the legal norms regulating relations in the sphere of the cyberspace and defining the law enforcement agencies functions including the cyberpolice in order to improve the efficiency of administration**.**

Target of research. The purpose of the study is to research and analyze the theoretical basis, legislative acts, and practical experience of foreign countries in order to outline main problems of the activities of the cyberpolice in Ukraine, to find ways to improve the situation of control and prevention of cybercrime in the country and to improve Ukrainian legislative framework.

Analysis of recent researches and publications. The following scientists analyze separate aspects of the question in their researches: K. Belyakov, I. Bykov, S. Bitko, V. Butuzov, O. Volevodz, V. Golubev, D. Dubov, S. Klyotskin, V. Milashev, M. Myronyuk, V. Mokhor, Y. Ryzhkov, T. Tropina, V. Khakhanovskyi, O. Pronevych, V. Shadrin and others.

Article's main body. An absolute world innovation leader for legal support of the cybersecurity is the United States of America (hereinafter – the US) where the matter of priority was the adoption of a number of laws and directives, that regulate activities in the cyberspace, among which the main position is occupied with the «Department of Defense Strategy for Operating in Cyberspace July 2011» [1]. In April, 2015, the updated cybersecurity strategy of the country was already released, which aims to guide the development of cyber forces of the Department of Defense (hereinafter -the DoD) and enhance cyber information resources. According to the Strategy there are three primary cyber missions: defending networks, systems, and information of strategic importance; defending the US homeland and US national interests against cyber attacks of significant consequence; providing cyber support to military operational and contingency plans. The strategic goals are the following:

– to build and maintain ready forces and capabilities to conduct cyberspace operations;

– to defend the DoD information network, secure DoD data, and mitigate risks to DoD missions;

– to be prepared to defend the US homeland and US vital interests from disruptive or destructive cyber attacks of significant consequence;

– to build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages;

– to build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability [2].

The key is that around these three missions and five goals the doctrine of cyber security is being built in the next five years.

Following the US cybersecurity strategies were adopted in the number of European countries, such as Sweden, Estonia, Slovakia, Czech Republic, France, Germany, Lithuania, Poland and others. Through the course of these strategies, the governments of the countries plan to bring greater understanding and transparency of each nation's military doctrine, policy, roles and missions in cyberspace; to strengthen international alliances and partnerships in the sphere of cyber security; to develop decisions for prevention the spread of harmful programs, etc. It is clear that cyber security is a problem which becomes more relevant with each passing year and is recognized as one of the most important in the world.

In March 15, 2016, the President of Ukraine signed the Decree, which introduced into force the decision of the National Security and Defense Council of Ukraine of January 27, 2016 «On the Cyber Security Strategy of Ukraine». Thus at the state level a common view of how to respond to threats in the informational sphere was formed. As other countries Ukraine faces the increasing trend of using cyberspace by the intelligence agencies, special military structures, terrorists, and criminals. But cyber security policy and strategy are just basic approaches, guidelines and key priorities of the country. These documents are general in nature, and their provisions should be supported by concrete acts. State cybersecurity policy should be conducted systematically and based on the experience of the countries, which in their turn have already passed this way, and only through cooperation with them it is more likely to prevent cyber threats and in case of occurrence to neutralize them.

A bright example to follow is the Czech Republic, where on February 16, 2015, a new National Cyber Security Strategy for the period from 2015 to 2020 was adopted. Besides the main directions of state policy this document outlines the functions of the subjects of national security in this area, including cyber police and it occupies a prominent place. The main task of the cyber police of the Czech Republic according to the strategy is to support capacity building of the police to investigate and prosecute the crime information. It should be noted that the vast majority of the tasks of the previous strategy has already been successfully completed. Two important achievements reached on the basis of the previous strategy are adopting the Act on Cyber Security and opening in May 2014 the National Cyber Security Centre including a fully operational Government Computer Emergency Response Team for cyber security incidents handling. The Strategy outlines the Czech Republic's vision of the cyber security field and defines the basic principles followed by the state in view of ensuring its cyber security, including protection of fundamental human rights and freedoms and of the democratic rule of law principles, comprehensive approach to cyber security based on principles of subsidiarity and cooperation, trust building and cooperation among public and private sector, and civil society, cyber security capacity building [3].

It is pleasant to note that the National Security and Defense Council of Ukraine decided to create a new structure in its working body – the National Cybersecurity Coordination Center.

The main regulatory and legal acts of the Republic of Lithuania in the sphere of national and cyber security are National Security Strategy (2012), The Military Strategy of the Republic of Lithuania (2012), Programme for the Development of Electronic Information Security for 2011–2019 (2011), Cybersecurity Act (2014). According to the Lithuanian national cyber security strategy secure cyberspace (i.e. assurance of electronic information security (cyberspace) security) is the concern of all entities whose activities are related to the provision of services in cyberspace (public institutions, private economic entities, academic society and others). Electronic information security (cyberspace security) projects implemented in cooperation enable the achievement of protection of all stakeholders' interests [4]. On January 1, 2015, National Cyber Security Centre, as a division of the Ministry of National Defense of the Republic of Lithuania started working to lead the country's effort to safeguard its information resources and infrastructure. The establishment of the centre was determined by the Law on Cyber Security and the amendments to relevant legislation.

As in most Europeans countries cybercrime legislation in Poland includes Cyberspace Protection Policy of the Republic of Poland (2013), National Security Strategy of the Republic of Poland (2014), and Cybersecurity Doctrine of the Republic of Poland (2015). Thus, the most recent legal act is Cybersecurity Doctrine of the Republic of Poland, which outlines further lines of work on improving national security in cyberspace and maps out tasks for state institutions, notably security agencies

and armed forces, private sector and non-governmental organizations. The document points out the need for pursuing active cyber defense, including offensive actions in cyberspace, and maintaining readiness for cyberwar, protection and defense of Polish teleinformational systems and accumulated data, and supporting key private firms in their cybersecurity efforts [5].

According to the Cyber Security Strategy of Ukraine the National Police of Ukraine is among the main components of the national cyber security system, which is primarily responsible for the protection of the rights and freedoms of the man and the citizen, interests of the society and the state from criminal attacks in the cyberspace; prevention, suppression and detection of cybercrime; raising public awareness about security in the cyberspace, etc [6]. The National Police of Ukraine consist of six departments: police patrol, police protection, criminal police, police of special purpose (KORD), pre-trial investigation bodies and special police.

As a part of the criminal police cyber police of Ukraine fulfill seven main objectives, namely the implementation of the state policy on combating cybercrime; combating cybercrime (skimming, cash trapping, credit card fraud, unauthorized debiting of bank accounts by means of remote banking, phishing, online fraud, piracy, card sharing, social engineering, malware, illegal content, refiling); advance informing people about new cybercrime; implementation of software for organizing and analyzing information on cyber incidents, cyber threats and cybercrime; respond to requests of foreign partners, delivered through networks of national contact points, which are available round the clock; participation in professional development of police officers on the use of computer technology in combating crime; participation in international operations and collaborate in real time; support of a network of contact points in 90 countries of the world [7]. But the formulation of the main objectives to be fulfilled by the cyber policemen should be supported by the adoption of a number of regulations at government level, which clearly regulate and explained in details all approaches, algorithms and procedures for the implementation of the main tasks of the special units.

On April 18, 2016 the Committee on Legislative Support of Law Enforcement of Verkhovna Rada of Ukraine recommended to adopt the draft law «On amendments to some laws of Ukraine concerning strengthening the responsibility for offenses committed in the field of information security and cybercrime». Relevant changes are expected to introduce into a number of legislative acts, including the Code of Ukraine on Administrative Offences, the laws of Ukraine «On Operative Search activities», «On the Security Service of Ukraine», «On Counterintelligence Activities», «On the National Security of Ukraine», «On Intelligence Services», «On Telecommunications» [8]. As a result of adoption of the draft law a legal and regulatory base in the sphere of law enforcement and special bodies will be improved, new terms «cyberspace» and «cybersecurity» will be introduced and fixed at the legislative level, functions of the subjects providing cybersecurity will be defined [9].

Conclusions and prospects for the development.

These are only the first attempts to improve Ukrainian legislation and they, unfortunately, cannot cover everything. It would be advisable to supplement the Law of Ukraine «On the National Police of Ukraine» with a separate partition «Ensuring cyber security», which would include principles of the process and define cyber powers of cyberpolicemen. Amendments are also required in Section 5 of the mentioned law in the form of additional articles clarifying the procedure for ensuring cybersecurity, including technical measures, and their implementation. While improving the legislative framework which regulates the activities of the police in Ukraine in general and cyberpolice in particular, one will certainly need to take into account the experience of the foreign countries, especially the United States, the Republic of Lithuania, the Republic of Poland, the Czech Republic, where existing laws operate, cyber police activities are meticulously regulated and fixed in the current legislation, and the experience of these countries can be applied to prevent possible errors in the future. Further study of this issue will help to bring domestic legislation in the sphere of policing in line with the international standards.

SOURCES

1. Department of Defense Strategy for Operating in Cyberspace July 2011 [Electronic resource]. – Access: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.
2. Cyber Strategy. U. S. Department of Defense [Electronic resource]. – Access: http://archive.defense.gov/home/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.
3. National Cyber Security Strategy for the period from 2015 to 2020 [Electronic resource]. – Access: https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_en.pdf.
4. The Programme for the Developmen of Electronic Information Security (Cyber Security) for 2011–2019 [Electronic resource]. – Access: http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf.

5. Cybersecurity Doctrine of the Republic of Poland [Electronic resource]. – Access: http://en.bbn.gov.pl/en/news/400,Cybersecurity-Doctrine-of-the-Republic-of-Poland.html.
6. Cyber Security Strategy of Ukraine [Electronic resource]. – Access: http://zakon2.rada.gov.ua/laws/show/96/2016.
7. Cyber police will be created in Ukraine, – Avakov [Electronic resource]. – Access: http://censor.net.ua/photo_news/355818/v_ukraine_budet_sozdana_kiberpolitsiya_avakov_infografika.
8. The Committee on Legislative Support of Law Enforcement recommends to adopt the draft law «On amendments to some laws of Ukraine concerning strengthening the responsibility for offenses committed in the field of information security and cybercrime» [Electronic resource]. – Access: http://iportal.rada.gov.ua/news/Novyny/128335.html.
9. Draft Law «On amendments to some laws of Ukraine concerning strengthening the responsibility for offenses committed in the field of information security and cybercrime» [Electronic resource]. – Access: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55668.

Х. В. СОЛНЦЕВА

кандидат юридичних наук, доцент кафедри адміністративного права та адміністративної діяльності Національного юридичного університету імені Ярослава Мудрого

ПОЛІЦІЯ ЯК СУБ'ЄКТ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

У статті розглядаються актуальні питання державної політики у сфері кібербезпеки та кіберзлочинності на прикладі країн Європи і Сполучених Штатів Америки, досліджується законодавство ряду зарубіжних країн, охоплюються проблеми правового регулювання кіберсфери в Україні і шляхи вдосконалення чинного законодавства України.

Дослідження в області кіберполіції набули особливої актуальності в Україні останнім часом, особливо після підписання Президентом України Указу, який ввів в дію рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України», єдиного на сьогоднішній день законодавчого акта, що регулює діяльність правоохоронних органів у цій сфері. Такий крок сприяє створенню умов для безпечного використання кіберпростору в інтересах людей, суспільства і держави. Вивчення і застосування успішного досвіду зарубіжних країн, таких як США, Литва, Польща, Чехія, має важливе значення в цілях вдосконалення законодавчої бази країни та діяльності української кіберполіції.

Ключові слова: поліція, діяльність кіберполіції, кіберзлочинність, стратегія кібербезпеки.

К. В. СОЛНЦЕВА

кандидат юридических наук, доцент кафедры административного права и административной деятельности Национального юридического университета имени Ярослава Мудрого

ПОЛИЦИЯ КАК СУБЪЕКТ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

В статье рассматриваются актуальные вопросы государственной политики в сфере кибербезопасности и киберпреступности на примере стран Европы и Соединенных Штатов Америки, исследуется законодательство ряда зарубежных стран, охватываются проблемы правового регулирования киберсферы в Украине и совершенствования действующего законодательства Украины.

Исследования в области киберполиции получили особую актуальность в Украине в последнее время, особенно после подписания Президентом Украины Указа, который ввел в действие решение Совета национальной безопасности и обороны Украины от 27 января 2016 г. «О Стратегии кибербезопасности Украины», единственного на сегодняшний день законодательного акта, регулирующего деятельность правоохранительных органов в этой сфере. Такой шаг способствует созданию условий для безопасной эксплуатации киберпространства и его использования в интересах людей, общества и государства. Изучение и использование успешного опыта зарубежных стран, таких как США, Литва, Польша, Чехия, имеет важное значение в целях усовершенствования законодательной базы страны и деятельности украинской киберполиции.

Ключевые слова: полиция, кибердеятельность полиции, киберпреступность, киберстратегии.