JEL codes: K 140, H 560, H 790

Sylwia Gwozdziewicz,
PhD (legal science), Department of Administration and National Security, The Jacob of Paradies University in Gorzów Wielkopolski. President, International Institute of Innovation Science-Education-Development in Warsaw, Poland, 66-400, Gorzów-Wielkopolski, Str. Teatralna, 25, tel.: +48690-900-994, e-mail: sylwiagwozdziewicz@gmail.com
ORCID: 0000-0003-3034-2880

Сільвія Говоздевич,
доцент (юридичні науки), Відділ Адміністрації і Нацбезпеки, Академія ім. Якова з Парадижа в Гожові Велькопольскому. Голова Міжнародного Інституту Інновацій Наука-Освіта-Розвиток у Варшаві, Польща, 66-400, Гожув-Велькопольский, вул. Театральна, 25, тел.: +48690-900-994, e-mail: sylwiagwozdziewicz@gmail.com
ORCID: 0000-0003-3034-2880

Сильвия Говоздевич,
доцент (юридические науки), Отдел Администрации и Нацбезопасности, Академия им. Якова с Парадижа в Гожове Велькопольском. Председатель Международного Института Инноваций Наука-Образование-Развитие в Варшаве, Польша, 66-400, Гожув-Великопольский, ул. Театральная, 25, тел.: +48690-900-994, e-mail: sylwiagwozdziewicz@gmail.com
ORCID: 0000-0003-3034-2880

Jakub Jakubowski,
Student Faculty of National Security, Department of Administration and National Security, The Jacob of Paradies University in Gorzów Wielkopolski, Poland, 66-400, Gorzów-Wielkopolski, Str. Teatralna, 25, tel.: +48723-49-50-49, e-mail: jakupofski@gmail.com
ORCID: 0000-0003-2367-5919

Якуб Якубовскі,
студент, Відділ Адміністрації і Нацбезпеки, Академія ім. Якова з Парадижа в Гожові Велькопольскому, Польща, 66-400, Гожув-Велькопольський, вул. Театральна, 25, тел.: +48690-900-994, e-mail: sylwiagwozdziewicz@gmail.com
ORCID: 0000-0003-2367-5919

Якуб Якубовски,
студент, Отдел Администрации и Нацбезопасности, Академия им. Якова с Парадижа в Гожове Велькопольском, Польша, 66-400, Гожув-Велькопольский, ул. Театральная, 25, тел. +48723-49-50-49, e-mail: jakupofski@gmail.com
ORCID: 0000-0003-2367-5919

THE TASKS OF THE NATIONAL ADMINISTRATION WITHIN THE PROTECTION OF THE POLISH CYBERSPACE

Abstract. The protection of the Polish cyberspace consists of numerous administrative tasks beginning from creating strategies, normative acts, next implementing them into force, arranging trainings concerning cyber safety, controlling particular institutions, enterprises and citizens, international cooperation and constant development in that matter. As for now, (pursuant to the report of the Supreme Audit Office from 2015) the Polish cyberspace is not protected properly. The report indicates committed mistakes of national entities but it also provides guidelines for better performance of the tasks within the Polish cyberspace protection. The supplementation to the guidelines for public administration in that matter will be implementation of the solutions of the new NIS Directive [2] of the UE Parliament and Council concerning funds for high common level of network and IT system security throughout the EU.

Keywords: the Polish cyberspace, public administration, cybercrime, MC (Ministry of Digital Affairs), UKE (Office of Electronic Communications), CERT (The Governmental Computer Emergency Response Team, MON (Ministry of National Defense).

ЗАВДАННЯ ДЕРЖАВНОЇ АДМІНІСТРАЦІЇ У СФЕРІ ОХОРОНИ КІБЕРПРОСТОРУ РП

Анотація. Охорона кіберпростору Польської Республіки складається з широкої гами адміністративних завдань, починаючи від створення стратегії, нормативних актів, потім впровадження їх у життя, ведення підготовок у сфері кібербезпеки, контролю окремих установ, підприємств і громадян, міжнародної співпраці, а також безперервного розвитку в цій сфері. Зараз (згідно з доповіддю найвищої Кімнати Контролю з 2015 р.) кіберпростір Польської Республіки не захищається у відповідний спосіб. Доповідь вказує на помилки державних суб'єктів, а також подає настанови для кращої реалізації завдань у сфері охорони кіберпростору РП. Доповненням настанов для державної адміністрації у цій сфері буде імплементація і впровадження рішень нової Директиви NIS Парламенту і Ради ЄС у справі засобів в ін-

тересах високого загального рівня безпеки мережі і систем інформатики на території Євросоюзу.

Ключові слова: кіберпростір РП, державна адміністрація, кіберзлочинність, MC, UKE, CERT, MON.

ЗАДАНИЯ ГОСУДАРСТВЕННОЙ АДМИНИСТРАЦИИ В СФЕРЕ ОХРАНЫ КИБЕРПРОСТРАНСТВА РП

Аннотация. Охрана киберпространства Польской Республики состоит из широкой гаммы административных заданий, начиная от создания стратегии, нормативных актов, потом внедрение их в жизнь, ведение подготовок в сфере кибербезопасности, контроля отдельных учреждений, предприятий и граждан, международного сотрудничества, а также непрерывного развития в этой сфере. Сейчас (согласно докладу наивысшей Комнаты Контроля с 2015 г.) киберпространство Польской Республики не защищается в соответствующий способ. Доклад указывает на совершенные ошибки государственных субъектов, а также подает наставления для лучшей реализации заданий в сфере охраны киберпространства РП. Дополнением наставлений для государственной администрации в этой сфере будет имплементация и внедрение решений новой Директивы NIS Парламента и Совета ЕС по делу средств в интересах высокого общего уровня безопасности сети и систем информатики на территории Евросоюза.

Ключевые слова: киберпространство РП, государственная администрация, киберпреступность, MC, UKE, CERT, MON.

The purpose of the article. Functioning of the most essential elements of a state critical infrastructure (i. e. systems connected with power, gas or water supply infrastructures) has been based on using IT solutions. The above factors show that stability, development and, first of all, state security depends on the level of cyberspace safety. Technology advance and development of IT systems have simultaneously led to occurring new forms of dangers resulting in consequences that are difficult to presume. Such dangers are as follow: cybercrime, cyber espionage and cyberterrorism or cyber war which are particularly dangerous for international security. In the time of common computerization, it is easy to imagine a scenario where cybercriminals could paralyze systems of critical infrastructure, world's financial markets, acquire access to bank accounts, steal secret intelligence information or take over control over a state telecommunication system. The events in Georgia, Estonia or Iran show the actions of cyber terror or cyber war character are a real threat nowadays. Operational tasks in that matter aim at reaching a strategic objective which is providing an acceptable level of security in the Polish cyberspace should be performed by the public sector entities (in the national

and international dimensions), private (commercial one), civic and in the trans-sector dimension. This article describes the tasks of the public sector in that matter.

Analysis of recent research and publications. The statement of basic materials. In present world, IT systems are foundations of proper activity of the most important areas of citizens, public sector functioning as well as the condition of a state development. The tendency to expand IT will undoubtedly increase quickly. Investments in digitization of economy and society are a basic requirement of global competition. The above factors show that stability and development, and first of all, security of present states depends on the level of cyberspace safety.

Cyberspace means "space of information transformation and exchange created by IT systems together with links between them and relations with users" [6]. Main features of cyberspace are: global range, easy access, efficiency, universality, relatively "decent price" which make areas of activity of governments, companies and persons are transferred into cyberspace. Today's digital technologies undoubtedly appear in every area of our lives. A completely new phenomenon is rapidly developing "cyberspace of devices" where the exchange of information is not performed between people but between devices. Such dialogues occur practically beyond users' awareness, besides facilitating exploitation and decreasing costs of service, they also become a source of increasing threat. A basic division of threats occurring in cyberspace is connected with objectives of individuals or organizations. According to that criterion, there may be the following cyber threats [6]:

• Cyber spies — they work for business of powerful resorts, they act in cyberspace in order to secretly acquire knowledge of press impact. Many countries such as China, the USA or Russia widely use cyberspace to collect economic and technology information.

• Cyber activists — they act in order to support some idea, they aim at its dissemination thanks to spectacular actions of great range that may undermine somebody's image.

• Cyber criminals — they act in order to acquire material benefit, they commit classical forgery or extortion thanks to measures, methods and devices available in cyberspace.

• Cyber terrorists — they act in cyberspace to support their political objectives, they aim at them by intimidation and arousing a state of threat. They also use cyberspace as a device of communication, propaganda, collecting funds and recruiting or training.

• Cyber soldiers — hire organizations or military divisions destined to perform military actions in cyberspace treated as another theatre or war actions. They may be performed individually or in cooperation with armed forces of other kind.

• Cyber bullies — they act in order to check or prove their skills, take revenge on adversary or former employer.

The division is agreed character only and in many cases a unanimous qualification of the threat sources is difficult or impossible.

According to Supreme Audit Office, the most popular threats in cyberspace are: using harmful software (viruses, worms, Trojan horses, back entrance,

espionage programs or procedures using known or secret gaps in commercial programs).

• Theft and using somebody else's personal data.

• Extortion, theft, forgery or destroying data.

• Blocking access to services (mailing bombs, overloading applications and services, mass appropriating computer systems in order to use them to conduct such overloading).

• Sending unnecessary or unwanted information.

• Social engineering attacks (extortion of information by pretending an institution or a friendly person).

• Advanced target attacks (performed via many coordinated and individualized methods aimed precisely at a particular person, organization or company).

Public administration satisfies collective and individual needs of citizens resulting from people's coexistence in a society, adopted by a state and performed by its bodies as well as local self-government entities [1]. Public administration consists of state (governmental) administration and self-government one. Both part perform state functions however and act for its benefit if we consider a unanimous system of law and state. One part performs it directly, the other one indirectly by self-government communities. Public administration has administrative power because a state has decided upon it in the act issued by it. The power dimension of power is always determined by legal regulations [12].

The role of public administration in fighting threats in cyberspace may arouse doubts because vast majority of infrastructure serving to the Polish cyberspace is in hands of commercial entities. Nevertheless, a necessary condition to guarantee cyber safety is building adequate legal system that would provide maintaining necessary and cohesive level of security by all key administrators and users of cyberspace.

Therefore, on 25th June 2013 the Council of Ministers adopted a document by resolution "The Policy of the Polish Cyberspace Security". All users of the cyberspace throughout Poland and abroad, where the representatives of Poland occur (diplomatic offices, military contingents) are the addressees of the above policy [5]. The strategic aim of the policy is acquiring an acceptable level of the cyberspace security in Poland by:

• decreasing results of IT incidents,

• increasing the IT infrastructure security,

• determining competences of particular entities,

• creating a cohesive cyberspace security management system,

• creating a system of coordination and exchange of information between entities,

• increasing cyberspace users' awareness.

The Polish cyberspace protection policy is aimed at the whole public administration — governmental administration and its central and local entities as well as at every level of self-government administration and other offices such as the offices of the President, Seym, Senate, National Broadcasting Council, and Spokesman of Children's Rights, National Bank of Poland or Polish Financial Supervision Authority. The public administration

tasks may be divided into those which concern all administration entities and those that refer to particular entities and particular situations. It would be difficult to put separate tasks to each entity because, due to the kind of competences, not all entities may be closely connected with the Polish cyberspace security, as for example Ministry of Digitization or Office of Electronic Communication.

A unit manager should create an information security management system in each public administration organizational unit basing on binding regulations and best know-how. It is assumed that a public unit will work out and modify as much as it needs and implement a security policy for IT systems used by them to perform public tasks. In order to provide cohesion of information security policies of organizational units, a proper minister of computerization with the agreement of Minister of National Defense and Head of Internal Security Agency may prepare guidelines concerning information security management systems [5].

There should be determined a role of proxy for cyberspace security within public administration organizational units whose tasks should include firs of all:

- preparation of emergency plans and their testing,
- implementing response procedures to computer incidents,
- identification and conducting frequent risks analysis,
- working out procedures providing informing proper CERT teams,
- performing duties resulting from legal regulations proper for providing cyberspace security.

A seat of the proxy for security is not indicated however the role of the proxy should be ascribed a person responsible for performing an IT security process. Besides, there should be educational actions implemented within cyberspace security among its users. Due to an inter-institutional type of the Polish cyberspace protection policy an entity supervising its realization is the Council of Ministers and an entity coordinating the realization is a proper minister of computerization. Obviously, the actions connected with cyberspace security should be performed by all public entities and units but there are about dozen entities that have a wider range of duties in that matter due to their kind.

The previously mentioned Ministry of Computerization (until 8th December 2015 Ministry of Administration and Computerization) plays a key role in the processes connected with the Polish cyberspace security. It is a proper body to communication, namely it is responsible for functioning regulations concerning security in network and information within telecommunication. It also plays a role of a proper body of computerization, including those resulting from the act from 17th February 2005 on computerization of entities performing public tasks. Ministry of Computerization plays a key role in the matter of IT society development and it played the role during the negotiations of the project of the NIS directive. The NIS Directive (the Directive of the EU Parliament and Council on the funds for high common level of network and IT system security in the EU) [2] which was adopted on 6th July 2016 by the European Parliament will

come into force in August. The regulations impose certain obligations onto the entities included in the directive, connected with providing cyber security; it assumes widening cooperation between EU members within cybersecurity. The Directive determines which duties within security shall key services operators be subject to (critical sectors such as power, transport, healthcare and finances) as well as suppliers of digital services (Internet trade platforms, search engines, cloud services). Each EU state shall be obliged to indicate a body or bodies to protect cyber security and work out a proper strategy.

The Directive establishes a common security level of network and information and strengthens cooperation between the EU members which shall help prevent from cybercrimes in future on important mutually connected European systems. Member states shall be obliged to create Computer Security Incident Response Teams as well. The Teams shall discuss trans-border security problems and ways of coordinated response. European Network and Information Agency (ENISA) shall play a key role in implementation of the directive particularly within coordinating cooperation between states within the CSIRT network.

Agency of Internal Security (ABW) shall be responsible for recognition, preventing and fighting threats aiming at the state internal security as well as defense and recognizing, preventing and detesting crimes aiming and the state security. ABW supervises protection of secret information.

The institution consists of

• Information Security Department (including CERT.GOV.PL)

• Anti-terrorist Centre (CAT)

• Department of Secret Information Security

Minister of the Interior is a proper minister for home affairs who plays a key role from the perspective of this dissertation concerning cyberspace security pursuant to art. 29 of the act from 4th September 1997 on public administration departments [11]. The home affairs department overwhelms such areas as: public order and security protection, emergency management, civil defense, border guarding. Proper minister for the interior supervises the activity of the Police, Border Guards, and Fire Brigades, Civil Defense of the State, Chairperson of Foreigners' Affairs, National Centre of Criminal Information and Office of Governmental Security. The Ministry of Interior conducts information systems and registers significant for state such as CEP, CEK, PESEL, ID register, passport register National Information System (KSI), it supervises IT systems such as Government Communication Network, TESTA, sTESTA, SIS, VIS and others. IT security of those systems is of significant importance for public administration functioning. [6].

The Police are a unit destined to fight crimes and one of its areas to combat crime is cyberspace. Since 2014 the Police have appointed special departments to fight cybercrime. They have aroused both in the Police Headquarter, Warsaw Police Station as well as in district police stations throughout Poland. As the Police website informs, the tasks of the department to fight cybercrime belong initiating and coordination of the Police actions within identifying main crime threats in the

Internet, cooperation with public institutions and public and private sector within acquiring information on methods and forms of crimes committed in cyberspace, working out types of cooperation with public sector entities, conducting multi source technical consultations and cooperation with national and foreign entities aiming at recognizing and implementing modern solutions in combating crime, implementing and maintaining dedicating IT systems, reviewing and working out suggestions of legislative changes within IT security, performing operational and recognizing actions in that matter [13].

Ministry of National Defense (MON) is one of the key entities acting in the area of the Polish cyberspace security. The main document that describes the Ministry's attitude to that matter is "The Strategy of the Polish National Security" pursuant to which one of the strategic objectives in the area of security is providing safe functioning of the Republic of Poland in cyberspace [7]. Appointing CERT was crucial for Ministry of National Defense acting for the MND purposes. In 2015 Computer Incident Response System (SRnIK) was established by the decision of the Minister of National Defense, used as acronym MIL-CERT PL in international contacts which was arranged in three-level structure. The Minister of National Defense also appointed a Proxy of the Minister of National Defense for Cyberspace Security by the decision No 38/MON from 16th February 2012. Substantial service of the Proxy is provided by the Coordinating Centre of Computer Incident Response System. MON also appointed a subject unit called the National Cryptology Centre (NCK) dealing mainly with research and implementation of cryptographic solutions for the purposes of public administration and army [15].

Ministry of Power, which is responsible for supervising implementation of the eIDAS resolution (until December 2015 it was the duty of Ministry of Economics), cannot be omitted while discussing the roles played by the particular public administration entities within the Polish cyberspace security. The main objectives is providing mutual respect and trans-border acceptance of electronic identification (eID) by the EU's member states, unification of legal frames to provide trust services and supervision over suppliers of those services in the EU and providing respecting trust services connected with electronic transactions [9].

Office of Electronic Communication (UKE), while playing the role of regulator of the mailing and telecommunication market provides implementation of the Telecommunication law in the context of cyberspace security. Its main tasks include affairs connected with reservation of waves for the purposes of radio and TV programs broadcasting, conducting contests for waves reservation for the purposes of radio or TV programs in a digital way, registering telecommunication entrepreneurs and analyzing proper markets as well as imposing, maintaining, changing or abolition of regulative obligations towards telecommunication entrepreneurs within supplying systems of conditioned access, electronic guides on programs and multiplexing of digital signals. UKE is supervised by the proper minister of communication (at

present it is the Minister of Digitization) [14].

Whereas Ministry of Justice, pursuant to art. 24 of the act from 4th September 1997 on public administration departments are responsible for the department of justice including the units: judiciary, prosecutor's office, notary office, advocacy and legal counsels in the matter resulting from separate regulations; performing punishments and educational measures, corrective measures ordered by courts and cases of post penitentiary assistance; free legal assistance mentioned in the act from 5th August 2015 on free legal assistance and legal education (Journal of Laws pos. 1255). The proper minister of justice affairs provides preparation of civil law codifying including penal and family ones [11]. In the matter of prosecuting cybercrime, the role of law enforcement authorities managing the law in that matter and supervising its proper performance is crucial do assuring appropriate order in virtual space.

Ministry of Finances (MF) is responsible for administration — public finances and significantly influences the final shape of budget opportunities referring to assuring cyberspace security as well. The services that are subject to that ministry are: The General Inspectorate of Financial Information, fiscal offices and chambers, fiscal audit offices including Fiscal Intelligence and Customs Service. MF and the subject services use the IT systems which are very important from the state financial system point of view (e. g. the e-declarations system). Attacks onto those systems may cause the biggest consequences for the state functioning and huge financial loss also for citizens.

Scientific and Academic Computer Network (NASK) should be mentioned as well, which is a research institute. It is supervised by Ministry of Science and Higher Education. NASK conducts numerous actions connected with cyberspace security affairs. The most important ones are as follow: appointing the first team of CERT kind in 1997 which has been working so far (CERT Polska) which de facto plays the role of the national CSIRT, appointing the team fighting dangerous and illegal contents in the Internet in 2005 (including CSAM), research activity within cyberspace security conducted together with the CERT Polska team and NASK, close cooperation with the EU's Agency for Network and Information Security– ENISA [9].

The Foreign Intelligence Agency is a public administration office however its activity is not overwhelmed by the range of public administration departments. The Agency is managed by the Head of the Foreign Intelligence Agency who is directly supervised by the Prime Minister. The tasks of the Agency are as follow: acquiring, analyzing and transferring information to proper entities that may be significant for security, recognizing and preventing from external threats, providing security of cryptographic communication with the Polish diplomacy and consular seats, messenger mailing, recognizing international terrorism and conducting electronic intelligence. At present, the activity of intelligence services of states is directed to IT technologies and actions in cyberspace. The Military Counterintelligence Service (SKW) is subject to MON and performs the tasks resulting from the act from 5th August 2010 on

the protection of secret information in relation to MON and subject units as well as to attaché's offices protection abroad within the range of personal security and industrial safety. SKW also certifies measures of electromagnetic protection, cryptographic devices and instruments serving to realization of IT security [15].

The Military Intelligence Service (SWW) is a special service, proper in the affairs of external threats protection for the state defense, combat security and ability of the Polish Military Forces and other organizational units subject to or supervised by the Minister of National Defense [9]. The service participates in information ad experience exchange between the NATO and EU's states intelligence services.

Conclusions. According to national reports published by the CERT response teams, EU's agencies or commercial companies dealing with cyberspace security, technology security threats (e.g. techniques of infecting with harmful software) are more and more advanced and the rage of incidents in cyberspace is growing every year. The problem of illegal and harmful contents in the Internet is increasing as well. The crime basing on illegal activity in cyberspace (e.g. phishing or crimes with the use of harmful software attacking e-bank accounts) is increasing as well. Such an image of the situation in cyberspace determines the necessity to conduct coordinated actions on the national level that shall involve both public administration and other interested parties. Another crucial matter is good cooperation between the particular offices and CERTs and constant exchange of information between the institutions including the trans-border information exchange. Nowadays, cyberspace security policy should be treated as priority. What does it look like in practice? The Supreme Audit Office negatively evaluated the realization of the tasks by the public entities within the Polish cyberspace protection in 2015. It claims that the public administration has net undertaken necessary actions so far aiming at providing the Polish cyber security. However, it should be considered that the Polish cyberspace security Policy is being still implemented. An important instrument of the legal "sign" in the cyberspace protection is the mentioned new EU's NIS Directive. Member states have 21 months for transposition of the directive regulations into national legal orders and extra 6 months for identification of the mentioned operators of key services.

At present, in Ministry of Digitization there are advanced works over the cyberspace strategy project for Poland as well as over a new act on the national system of cyber security. Both the strategy and the act shall perform requirements imposed by NIS.

REFERENCES

1. *Boć J.*, Prawo administracyjne, Wrocław. 2005. — 16 s.
2. *Dyrektywa* Parlamentu Europejskiego i Rady (UE) z 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium UE.
3. *Kańciak A.* Bezpieczeństwo w cyberprzestrzeni i społeczeństwo informacyjne jako przedmioty analiz naukowych i debat publicznych, Warszawa, 2013.

4. *Konstytucja* Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. 1997 nr 78 poz. 483).
5. *Polityka* ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, Ministerstwo Administracji i Cyfryzacji, Warszawa, 2013. — 8, 14 s.
6. *Realizacja* przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, Raport NIK, Warszawa, 2015. — 4, 20 s.
7. *Strategia* Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, 2014.
8. *System* administracji publicznej w Polsce, Ministerstwo Administracji i Cyfryzacji, Warszawa, 2014.
9. *System* bezpieczeństwa cyberprzestrzeni RP, NASK/CERT. — Warszawa, 2013. — 15, 20, 24, 27 s.
10. *Ustawa* z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r., poz. 1114).
11. *Ustawa* z dnia 4 września 1997 r. o działach administracji rządowej (t. j. Dz. U. z 2016 r. poz. 543, 749).
12. *Zimmermann J.* Prawo administracyjne, Wyd. IV, Wolters Kluwer. — Warszawa, 2010. — 26 s.
13. www.policja.pl
14. www.mc.gov.pl
15. www.mon.gov.pl