Illia Onyshchuk
West Ukrainian National University, Ukraine

The Reforming of State Service of Special Communication and Information Protection of Ukraine in the Context of Ukraine's Integration Into NATO

The next year after gaining independence of Ukraine, the President of Ukraine issued a Decree "About State Service of Ukraine for Technical Protection of Information", which establish the basis of their work. Meanwhile, as a legacy of the Soviet Union, there was the State Committee of Ukraine on State Secrets. However, this systemic dualism didn't run for a long time, and according to the Decree of the President of Ukraine "About changes in the system of central authorities" from 07.26.1996 №596/16 these institutions were eliminated and replaced on the State committee of Ukraine on State Secrets and technical protection of information[1].

Due to changing the political environment and lack single concept of this service, this Committee was dissolved in 2000. And all functions of technical protection of information and state secrets were transferred to certain departments of the Security service of Ukraine.

But on February 23, 2006, Verkhovna Rada of Ukraine (the supreme legislative body of Ukraine) adopted Law on State Service of Special Communication and Information Protection of Ukraine on the basis of Departure of special communication system and information protection of the Security service of Ukraine. And in this form with amendments, this State service still functions.

Today, the State Service for Special Communications and Information Protection of Ukraine has 17 departments and offices, which provide legal and administrative support, as well as directly perform the functions assigned to the Service[2].

---

[1] I.S. Zheveleva, Genesis of the activities of state security services regarding to the protection of restricted information of Ukraine, Електронне наукове фахове видання «Юридичний науковий електронний журнал», T. Kolomoyets, O. Bondar, M. Vikhlyaev, 2021, Zaporizhzhia http://lsej.org.ua/5_2021/5_2021.pdf p. 345.

[2] The official website of the State Service of Special Connection of Ukraine; https://cip.gov.ua/ua/news/onovlena-struktura-administraciyi-derzhspec-yazk, accessed: 22.11.2021.

Among the main tasks of the State Service for Special Communications and Information Protection of Ukraine are:

1) formation and implementation of state policy in the areas of cryptographic and technical protection of information, cybersecurity, protection of state information resources and confidential information providing government communications to the President of Ukraine, Chairman of the Verkhovna Rada of Ukraine, Prime Minister of Ukraine, other officials, local self-government bodies, military administration bodies, heads of enterprises, institutions and organizations in peacetime, in a state of emergency and in a special period;
2) counteraction to technical intelligence, as well as in the spheres of telecommunications, use of radio frequency resources of Ukraine;
3) organization of the system of electronic document management (in terms of information protection of state bodies and local governments), electronic identification (using electronic trust services), electronic trust services,
4) regulation of special-purpose postal service, government courier service;
5) ensuring the functioning of the government team for responding to computer emergencies in Ukraine CERT-UA[3].

Due to Russia's armed aggression in eastern Ukraine and the adoption of a strategic course on the EU and NATO in the Constitution of Ukraine, the issue of bringing the State Service for Special Communications and Information Protection to global standards has become extremely acute.

After 2013, a number of changes are made that expand and to some extent demilitarized this Service. If before that the State Special Service was more concerned with the functioning of the system of special communication between the President of Ukraine, the Cabinet of Ministers of Ukraine, the Verkhovna Rada, other executive bodies and local governments and courier services, the service was transferred to ensure the functioning of the National Telecommunication System between government agencies and agencies, the formation of policies to combat cyber threats, the establishment, and issuance of permits for technical protection of information and radio frequency, coordination of cybersecurity entities, functioning of the State Center for Cyber Defense.

Such steps are logical, as with the beginning of Russia's armed aggression in Crimea and eastern Ukraine, the number of cyberattacks on law enforcement information systems, the Ministry of Defense of Ukraine, the Armed Forces of

[3] Law «On the State Service for Special Communications and Information Protection of Ukraine», https://zakon.rada.gov.ua/laws/show/3475-15#Text, № 3475-IV, February 23, 2006, accessed: 19.11.2021.

Ukraine, websites of ministries, agencies, and electronic trust services and even critical infrastructure grew up[4].

The Microsoft Digital Defense Report for October 2021 states that between June 2020 and July 2021, Ukraine ranked second in the world (after the United States) in the number of cyberattacks received from Russia[5].

All this indicates the need to improve the protection of Ukrainian cyberspace and the need to reform the State Service for Special Communications and Information Protection of Ukraine in order to more effectively combat cyber threats from Russia and other unfriendly countries.

The Decision of the National Security and Defense Council, as well as the Decree of the President of Ukraine of October 22, 2021 approved the Concept of reforming the State Service for Special Communications and Information Protection of Ukraine[6].

According to this Concept, the process of reforming the Service will consist of 2 stages:

The first stage (January 2022 - December 2023) provides:

1) improvement of Ukrainian legislation on the organization and activities of the State Service for Special Communications and Information Protection of Ukraine, taking into account international standards and best world practices, in particular, in the field of information protection in information, telecommunications and information and telecommunications systems;
2) launching a wide range of research in the field of cybersecurity and development of applied systems and means of cybersecurity;
3) optimization of organizational structures of bodies and subdivisions of the State Service for Special Communications and Information Protection of Ukraine, taking into account certain functions and capabilities;
4) implementation of measures for the establishment and development of the State Service for Special Communications and Information Protection of Ukraine as a Security Accreditation Body, which organizes accreditation on security issues of all national communication and information systems in which NATO information is restricted;
5) further development of special communication systems, in particular in the interests of the network of situational centers of state bodies, de-

[4] The official website of the Ministry of Defense of Ukraine; https://www.mil.gov.ua/ukbs/kiberataki-rosijskoi-federaczii-hronologiya.html, accessed: 22.11.2021.

[5] Microsoft digital defense October 2021, p. 133. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi, accessed: 20.11.2021.

[6] The official website of the President of Ukraine; https://www.president.gov.ua/documents/5442021-40437, accessed: 20.11.2021.

ployment of the radio segment of the transport platform of the National Telecommunication Network;

6) reforming and developing systems of cryptographic and technical protection of information, counteracting technical intelligence, evaluating the effectiveness of implemented innovations.

The second stage (January 2024 - December 2025) provides:

1) modernization of the state system of government communication by integrating its networks into a single secure multiservice platform of the National Telecommunication Network and the transition to providing consumers with a wide range of modern services;
2) conducting accreditation on the security of national communication and information systems that process NATO information with limited access;
3) modernization of the system of special communication nodes of suburban control points of state bodies;
4) implementation of measures and development of cyber security tools based on the results of scientific research in the field of cybersecurity.

It follows from the text of the concept that the legislator seeks to continue the development of the State Service for Special Communications and Information Protection, which was established after 2013 - a departure from the standards of the Soviet Union and the Russian Federation and the transition to Euro-Atlantic practices. The aim of the Concept is to reform and develop the State Service for Special Communications and Information Protection of Ukraine as a subject of the security and defense sector with the introduction of a unified system of resource planning and management based on the modern experience of Europe and Euro-Atlantic countries.

So, I would like to draw your attention to the approaches to the organization of the service of our NATO partners Poland and the United States.

In the Republic of Poland, the system of counteracting cyber threats and special communications is organized according to a slightly different system. The Internal Security Agency (ABW Agencja Bezpieczeństwa Wewnętrznego) deals with special communication and information protection[7], the Polish Intelligence Agency (SWW Agencja Wywiadu)[8], and the National Research Institute (NASK)[9].

Each of them carries out its activities in accordance with the tasks assigned to them: the Internal Security Agency is primarily concerned with protecting civilians

[7] The official website of the Internal Security Agency; https://www.abw.gov.pl, accessed: 20.11.2021.

[8] The official website of the Intelligence Agency; https://www.sww.gov.pl, accessed: 20.11.2021.

[9] The official website of the National Research Institute NASK; https://en.nask.pl, accessed: 05.12.2021.

from possible threats, the Polish Intelligence Agency is engaged in providing cryptographic protection of communications of Polish diplomatic missions. However, I would like to focus on such a structure as NASK. NASK is a National Research Institute established under the Secretariat of the Prime Minister of Poland.

NASK carries out research and development projects focused on increasing the efficiency, reliability, and security of information and telecommunication networks and other complex network systems. What makes them stand out from strictly commercial businesses is their approach to developing solutions for the current and future needs of their clients. Commercial challenges are taken on from the perspective of science, and its tools, which are often broader and more abstract, whereby enabling them to achieve results that are not only satisfying but also innovative.

So one of the differences is the differentiation of these responsibilities between Polish law enforcement and civilian structures. Nevertheless, the Cyber Security Center (Centrum Cyberbezpieczeństwa) was established in Poland in 2016[10]. The center monitors threats, receives and handles cyber incidents, manages the mode of reporting network threats, and so on. This year, a similar UA: 30 centers with the CERT-UA team was established in Ukraine[11]. The experience of creating such centers is global and generally aimed at:

1) accumulation and analysis of data on cyber incidents, maintenance of the state register of cyber incidents;
2) providing practical assistance to the owners of cyber security facilities in preventing, detecting, and eliminating the consequences of cyber incidents on these facilities;
3) interaction with law enforcement agencies, ensuring their timely information about cyberattacks;
4) interaction with foreign and international organizations in response to cyber incidents, in particular in the framework of participation in the Forum of teams responding to security incidents FIRST with the payment of annual membership fees;
5) processing of information received from citizens about cyber incidents concerning cyber security objects, etc.

This Cybersecurity Center consists of 5 rapid response teams and all of them work in different directions, for example, The Cyber Threat Team of the Scientific and Academic Computer Network (CSIRT NASK) works directly with local gov-

[10] The official website of the Republic of Poland; https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa-, accessed: 23.11.2021.

[11] President Volodymyr Zelensky has opened the UA30 Cyber center, whose specialists are to prevent virtual attacks on Ukrainian facilities, Ukrinform 2021, https://www.ukrinform.ua/rubric-society/3244570-zelenskij-vidkriv-kibercentr-ua30.html, accessed: 23.11.2021.

ernments, legal entities, executive authorities, etc.; The Resistance Team of the Government of the Republic of Poland (CCIRT GOV) monitors the security of state bodies, state control bodies, and courts, etc.

Summarizing and comparing the experience of the Republic of Poland, I note the differences in the functioning and distribution of cyber security functions among law enforcement agencies and the lack of such an institution as the State Service for Special Communications and Information Protection in this country. However, the principles laid down in the Concept of reforming the State Service for Special Communications and Information Protection of Ukraine and the Cyber Security Strategy of the Republic of Poland 2019-2024 have a common vector of development and harmonization of these laws with EU and NATO requirements.

In the United States, the Cyber Security and Infrastructure Agency (CISA) is in charge of cybersecurity and the operation of the special communications system[12]. In my opinion, when writing the Law of Ukraine „On the State Service for Special Communications and Information Protection of Ukraine", legislators relied on the American experience of this service, because in terms of powers and structure of Ukrainian and American services are very similar.

CISA has the following tasks:

1) Ensuring the security of US cyberspace in a public-private partnership.
2) Creating a secure environment for critical infrastructure in both the physical and digital dimensions.
3) Support and improvement of the special communication network. Conducting special pieces of training and exercises for partners of all levels
4) Establishment and operation of a system of communication between US educational institutions, their provision of the Internet
5) Planning, analysis, and risk assessment of the US electoral system, information and telecommunications technology, development of 5th generation (5G) networks, etc.

As in Ukraine and Poland, there are 73 cyber threat response teams in the United States. But that's not the end of secure cyberspace, as much of the critical infrastructure is privately owned, and the CISA has created a National Risk Management Center that brings together the private sector, government, and other key stakeholders to identify and analyze, prioritization and management of the most significant risks in the US critical infrastructure.

Given the strong material and technical base, our partners from the United States do not stop there, and On May 12, President Biden signed Executive Order 14028, "Improving the Nation's Cybersecurity" to support the nation's cyberse-

[12] The official website of the Cybersecurity & infrastructure security agency https://www.cisa.gov/publication/cisa-fact-sheet, accessed: 23.11.2021.

curity and protect the critical infrastructure and Federal Government networks underlying nation's economy and way of life[13].

Interestingly, despite a fairly open society, this Decree actually expands the powers of the relevant authorities to control certain areas of relations. I think this is a bright marker for our country because even such a highly developed country as the United States sets stricter rules of conduct and control in its cyberspace:

1) Remove Barriers to Threat Information Sharing Between Government and the Private Sector
2) Modernize and Implement Stronger Cybersecurity Standards in the Federal Government
3) Establish a Cyber Safety Review Board
4) Improve Investigative and Remediation Capabilities

In this way, CISA receives a wider range of tools to combat cyber incidents and cybercrime, ensure the security of personal data of citizens of the United States and other countries, military facilities and critical infrastructure in general.

Since the State Service for Special Communications and Information Protection of Ukraine is structurally similar to CISA, the directions of activity and reform are identical, which allows me to conclude that the Concept complies with generally accepted Euro-Atlantic norms.

In conclusion, I would like to note that the reform of the State Service for Special Communications and Information Protection of Ukraine is a necessary step and one that will bring Ukraine even closer to full membership in the North Atlantic Alliance. The concept of reforming this service is generally in line with global norms and trends, and therefore will be able to guarantee the cybersecurity of every citizen of Ukraine in the future.

* * *

The Reforming of State Service of Special Communication and Information Protection of Ukraine in the Context of Ukraine's Integration Into NATO

(summary)

In this article, was analyzed the development of State Service of Special Communication and Information Protection of Ukraine during the period of independence of Ukraine, the necessity of reforming and Service, and the experience

[13] The official website of the President of the United States https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, accessed: 02.12.2021.

of Poland and the United States in this field: 1) The process of formation and general tasks of State Service of Special Communication and Information Protection of Ukraine, 2) The Conception of reforming of Service of Special Communication and Information Protection of Ukraine, 3) The experience of the United States and Poland in ensuring the country's cybersecurity.

Bibliography

Law «On the State Service for Special Communications and Information Protection of Ukraine»; https://zakon.rada.gov.ua/laws/show/3475-15#Text, № 3475-IV, February 23, 2006, accessed: 19.11.2021.

Microsoft digital defense October 2021, p. 133. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi, accessed: 20.11.2021.

President Volodymyr Zelensky has opened the UA30 Cyber center, whose specialists are to prevent virtual attacks on Ukrainian facilities, Ukrinform 2021, https://www.ukrinform.ua/rubric-society/3244570-zelenskij-vidkriv-kibercentr-ua30.html, accessed: 23.11.2021

The official website of the Cybersecurity & infrastructure security agency https://www.cisa.gov/publication/cisa-fact-sheet, accessed: 23.11.2021.

The official website of the Intelligence Agency; https://www.sww.gov.pl, accessed: 20.11.2021.

The official website of the Internal Security Agency; https://www.abw.gov.pl, accessed: 20.11.2021.

The official website of the Ministry of Defense of Ukraine; https://www.mil.gov.ua/ukbs/kiberataki-rosijskoi-federaczii-hronologiya.html, accessed: 22.11.2021.

The official website of the National Research Institute NASK; https://en.nask.pl, accessed: 05.12.2021.

The official website of the President of Ukraine; https://www.president.gov.ua/documents/5442021-40437, accessed: 20.11.2021.

The official website of the President of the United States https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, accessed: 02.12.2021.

The official website of the Republic of Poland; https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa- , accessed: 23.11.2021.

The official website of the State Service of Special Connection of Ukraine; https://cip.gov.ua/ua/news/onovlena-struktura-administraciyi-derzhspec-yazk, accessed: 22.11.2021.

Zheveleva I.S., Genesis of the activities of state security services regarding to the protection of restricted information of Ukraine, Електронне наукове фахове видання «Юридичний науковий електронний журнал», Kolomoyets T. Bondar O. Vikhlyaev M. 2021, Zaporizhzhia http://lsej.org.ua/5_2021/5_2021.pdf p. 345.