Public Policy and Accounting
ISSN 2707-9325

UDC 004.056.5:339.924(477)

Institutional and legal model for the formation and implementation of the state policy of combating cybercrime

Savchuk Serhii[1]

Applicant
Zhytomyr State Polytechnic University

Abstract

The development of digital technologies has significantly transformed the entire sphere of public life, while at the same time leading to a rapid growth in cybercrime, a phenomenon that includes cyberattacks on critical infrastructure, financial systems, government agencies and the private sector, which has become one of the key challenges of our time. Effective counteraction to cybercrime requires not only the improvement of technical solutions, but also the formation of a coherent institutional and legal model that combines legislative, organisational and managerial mechanisms. The article deals with the issues of forming and implementing the State policy of combating cybercrime on the basis of the institutional and legal approach. The author identifies the main elements of the model for the formation and implementation of the state policy of combating cybercrime, in particular, the legislative framework, the system of coordination between cybersecurity actors, and the mechanisms of international cooperation. Particular attention is paid to the analysis of national approaches to countering cyber threats. The author emphasises the need to strengthen legal and regulatory frameworks, develop a national cybersecurity strategy, and introduce modern information security technologies. A single coordinating body has been established to monitor and respond to cyberattacks, as well as to intensify international cooperation to share experience and counter transnational cybercrime.

Keywords: cybercrime; cyber threats; cybercrime; cyber defence; state policy; cybersecurity; hybrid warfare.

1. Introduction

In today's rapidly developing information and communication technologies, cybercrime is becoming one of the most serious challenges for the state, society and business. The rapid expansion of digital technologies, the increase in data volumes and their integration into all spheres of society create new security risks that require an urgent response from public authorities and governments. Cyberattacks on critical infrastructure, financial institutions, government agencies and private companies cause significant damage to the economy, undermine public confidence in government institutions and pose a threat to national security. In this context, there is a need to develop an effective institutional and legal model for the formation and implementation of the state policy on combating cybercrime and adaptation of national legislation to international standards. Successful counteraction to cybercrime requires coordination between state institutions, the private sector and civil society, as well as active international cooperation. The creation of an effective institutional and legal model will ensure an efficient cybersecurity management system, develop clear mechanisms for responding to cyber threats, strengthen preventive measures and increase the level of protection of public and private information.

Corresponding author:
[1] ORCID: https://orcid.org/0009-0007-7436-0702

doi: https://doi.org/10.26642/ppa- ppa-2023-2(8)-56-60

2. Literature review

The issues of state policy on combating cybercrime are the subject of research by a number of domestic and foreign scholars. In particular, V. Pavlenko believes that «...cybersecurity is an activity aimed at protecting systems, networks and computer programs from digital attacks» [1, p. 31]. A similar opinion is shared by O. Baranov, who states that '...cybersecurity is information security in the context of the use of computer systems and/or telecommunication networks. Or let's give a more detailed definition: cybersecurity is a state of protection of vital interests of an individual, society and the state in the conditions of using computer systems and/or telecommunication networks, which minimises damage to them due to: incompleteness, untimeliness and unreliability of the information used; negative information impact; negative consequences of information technology; unauthorised dissemination, use and violation of the integrity, confidentiality and availability of information' [2, p. 61]. Melnyk S., Tikhomirov O., Lenkov O. argue that «...cybersecurity can be defined as the protection of vital interests of a person and a citizen, society and the state, which ensures sustainable development of society, timely detection, prevention and neutralisation of real and potential threats to national interests in the field of information and telecommunication systems» [3]. Furashev V. argues that «...cybersecurity is a state of the ability of a person, society and the state to prevent and avoid directed, primarily unconscious, negative impact (management) of information» [4]. Shelomtsev V. insists that «...cybersecurity is a set of special subjects of cybersecurity, means and methods used by them, as well as a set of relevant interrelated legal, organisational and technical measures carried out by them» [5]. Despite the existence of numerous studies on cybersecurity issues, theoretical and methodological approaches to the formation and implementation of the state policy of combating cybercrime require additional substantiation.

3. Identification of previously unresolved issues and formulation of research hypotheses

Despite some progress in the study of cybersecurity and the fight against cybercrime, a number of aspects remain insufficiently researched. In particular, the absence of a comprehensive institutional and legal model of state policy in this area complicates coordination between various cybersecurity actors, including government agencies, private companies, and civil society. The issues of implementing international standards, strengthening legal regulation, and ensuring prompt response to cyberattacks remain unresolved. Additional challenges are associated with the dynamic development of cyber threats and the need to adapt to new technologies used for criminal purposes.

The research hypotheses are as follows:

- creating an institutional and legal model that integrates national and international mechanisms for combating cybercrime will help to increase the effectiveness of state policy in the field of cybersecurity;
- strengthening coordination between cybersecurity actors through the introduction of a unified approach to risk management and response to cyber threats will reduce the level of cybercrime;
- improving legislation by making it more focused on modern cybercrime challenges will ensure more effective protection of critical information infrastructure and stakeholder interests.

4. Methodology and research methods

The study is based on a systemic approach which allows considering the institutional and legal model of countering cybercrime as an integral system that includes legal, organisational, technological and social components. The research methodology includes an interdisciplinary analysis of legal, managerial, technical, and socio-economic aspects related to countering cybercrime. To achieve the research objective, the following methods are used: system analysis - to study the components of the state policy in the field of cybersecurity and their interrelationships; content analysis - to assess the current legislation, international regulations and cybersecurity strategies; comparative analysis - to compare international practices of combating cybercrime and identify opportunities for their adaptation to Ukrainian realities.

5. Main results

The analysis of the powers of the current supreme and central authorities in Ukraine allowed us to determine the composition of the subjects of governance in the field of countering cybercrime. The President of Ukraine, according to the Constitution of Ukraine and the Law of Ukraine «On National Security of Ukraine» [6, 7]: guarantees the national security of the country as a whole and its components, including cybersecurity; heads the National Security and Defence Council of Ukraine, which deals with national security issues in general and cybersecurity in particular; approves or vetoes legislative acts adopted by the Verkhovna Rada of Ukraine (including those related to cybersecurity and countering cybercrime).

The Verkhovna Rada of Ukraine has the following powers within the framework of public administration in the field of countering cybercrime according to national legislation [6–8]: it adopts laws of Ukraine, including those related to cybersecurity and countering cybercrime; oversees the activities of the Cabinet of Ministers of Ukraine, including in the field of cybersecurity and countering cybercrime. The National Security and Defence Council of Ukraine has the following powers in the field of cybersecurity and cybercrime management [9]: «... develops and considers at its meetings issues related to national security in

general and cybersecurity in particular and submits proposals to the President of Ukraine, makes decisions on: determining the strategic national interests of Ukraine, conceptual approaches and directions of ensuring cybersecurity...».

The Cabinet of Ministers of Ukraine, in turn, within the framework of public administration of countering cybercrime [10]: «ensures the implementation of the state policy, the implementation of the Constitution and laws of Ukraine, acts of the President of Ukraine in the field of cybersecurity and countering cybercrime; carries out measures to ensure cybersecurity of Ukraine, fight against cybercrime; directs and coordinates the work of ministries and other executive authorities involved in the process of managing cybercrime».

The State Service for Special Communications and Information Protection is responsible for [11]: «the formation and implementation of state policy in the field of cyber defence, ... active counteraction to aggression in cyberspace; implementation of the state policy on the protection of critical technological information, cyber defence of critical information infrastructure facilities, and state control in these areas; development of general requirements for cyber defence of critical infrastructure facilities; establishing and ensuring the functioning of the system of active counteraction to aggression in cyberspace; establishing and ensuring the functioning of the Centre for Active Counteraction to Aggression in Cyberspace; performing other tasks stipulated by the legislation in the field of cybersecurity and cyber defence».

The National Police of Ukraine performs the following tasks within the framework of state administration of countering cybercrime [12]: «conducts various activities to prevent the commission of cybercrime...». The Security Service of Ukraine has the following powers under the law [13]: «carries out information and analytical work in the interests of the effective conduct of internal and external activities related to the cybersecurity of Ukraine by the state authorities and management of Ukraine; carries out counterintelligence measures to ensure the cybersecurity of our state's entities abroad; detects, stops and solves criminal cyber offences...».

The State Bureau of Investigation, according to the national legislation, exercises the following powers within the framework of state administration of cybersecurity [14]: «participates in the formation and implementation of state policy in the field of combating cybercrime, submits relevant proposals to the Cabinet of Ministers of Ukraine; carries out information and analytical measures to establish the systemic causes and conditions of organised cybercrime, takes measures to eliminate them; stops and solves relevant criminal cyber offences; carries out operational and search activities and pre-trial investigation of relevant criminal cyber offences».

The Ministry of Internal Affairs of Ukraine, in turn, is vested with the following powers in the field of combating cybercrime in accordance with the law [15]: «ensures the formation of state policy in the field of combating cybercrime, as well as the provision of police services». The Ministry of Information Policy of Ukraine ensures the formation and implementation of state policy in the field of information security [16]: «is the main body in the system of central executive bodies that ensures the formation and implementation of state policy in the areas of culture, state language policy, promotion of Ukraine in the world, state foreign broadcasting, information sovereignty of Ukraine (in terms of powers to manage integral property complexes of the state enterprise Multimedia Broadcasting Platform of Ukraine and the Ukrainian National News Agency Ukrinform) and information security, and also ensures the formation and implementation of state policy in the areas of restoration and preservation of national memory, arts, protection of cultural heritage, museums, export, import and return of cultural property».

The growing volume of cybercrime in general and in the context of martial law, which is also related to aggression against Ukraine and malicious acts of the enemy, necessitates the establishment of a separate central executive body of a law enforcement nature, which should be entrusted with the tasks of combating cybercrime and protecting cybersecurity – the State Bureau of Cybersecurity. In view of the above and the previously formed composition of the functions of state administration of countering cybercrime: The President of Ukraine carries out organisational, institutional, security and protection functions; the Verkhovna Rada of Ukraine – organisational, institutional, security, protection and control functions; The National Security and Defence Council of Ukraine, the State Service for Special Communications and Information Protection – forecasting and planning, organisational, institutional, security, protection, and control functions; the Cabinet of Ministers of Ukraine – forecasting and planning, governing, organisational, institutional, security, information, and economic functions; The State Bureau of Cyber Security, the National Police of Ukraine, the Security Service of Ukraine, the State Bureau of Investigation – forecasting and planning, management, organisational, control, institutional, operational, protective, security, information, economic, legal functions; the Ministry of Internal Affairs of Ukraine and the Ministry of Information Policy of Ukraine – forecasting and planning, organisational, control functions.

The institutional mechanism of public administration to counter cybercrime looks like this (Fig. 1). Implementation of this mechanism in practice will increase the effectiveness of the fight against cybercrime and improve the level of cybersecurity of the country. Its expansion is based on the need to establish the State Bureau of Cybersecurity, which, unlike the Cyber Police of the National Police of Ukraine, will have broader functions related to cybercrime, which are particularly serious and affect the national security of the state. The tasks of the State Bureau of Cybersecurity are proposed to include: identifying risks and threats to the country's cybersecurity, assessing them, and minimising and eliminating them; development of measures to harmonise the national system of combating cybercrime with EU directives; drafting proposals for regulatory acts on the prevention of cybercrime in the system of threats to the national security of the state; achieving the country's cybersecurity by preventing, detecting, suppressing, and investigating cybercrime; summarising and analysing information on cybercrime and identifying means of preventing it in the future; planning measures to counter cybercrime; and formulating analytical conclusions.

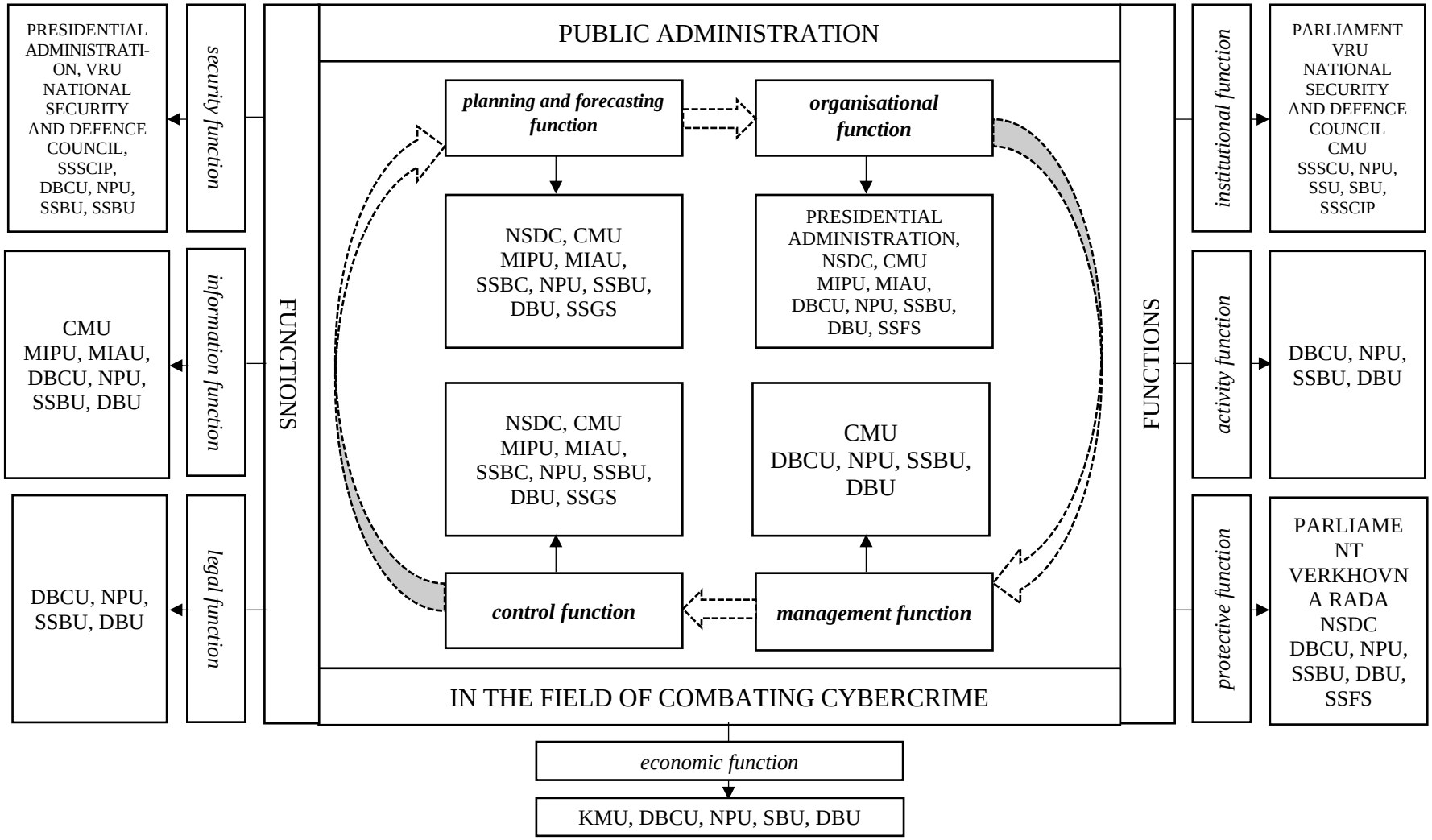

Fig. 1. Institutional mechanism of public administration in the field of countering cybercrime

Source: developed by the author.

To ensure the high efficiency of the State Bureau of Cybersecurity, its powers should be defined, in particular: direct interaction with the EU cybersecurity actors; both in terms of investigating cybercrime and harmonising state policydirect cooperation with international police organisations, in particular Interpol and Europol, in terms of combating cybercrime and other types of crimes related to the use of information technology; cooperation with the State Service for Special Communications and Information Protection in terms of technical support for ensuring the state's cybersecurity and investigating cybercrime; conducting or participating in special checks of persons applying for senior positions in the public administration system or other positions with a high level of corruption risk; direct interaction with the National Anti-Corruption Bureau of Ukraine in terms of investigating corruption offences related to cryptocurrencies; cooperation with law enforcement agencies of the European Union in the investigation of cybercrime as a transnational crime; participation in temporary investigative teams to investigate crimes that pose a threat to national security; preparation of analytical reports for the President of Ukraine, the Prime Minister of Ukraine, the Chairman of the Verkhovna Rada of Ukraine on the state of cyber threats and their impact on the national security of Ukraine.

6. Conclusions

Thus, the study contributed to the development of institutional provisions of public administration in the field of countering cybercrime through the formation of the institutional mechanism of the latter, in which: The President of Ukraine carries out organisational, institutional, security, and protective functions; the Verkhovna Rada of Ukraine - organisational, institutional, security, protective, and control functions; The National Security and Defence Council of Ukraine, the State Service for Special Communications and Information Protection - forecasting and planning, organisational, institutional, security, protection, and control functions; the Cabinet of Ministers of Ukraine - forecasting and planning, governing, organisational, institutional, security, information, and economic functions; The State Bureau of Cyber Security, the National Police of Ukraine, the Security Service of Ukraine, the State Bureau of Investigation - forecasting and planning, management, organisational, control, institutional, operational, protective, security, information, economic, legal functions; the Ministry of Internal Affairs of Ukraine and the Ministry of Information Policy of Ukraine - forecasting and planning, organisational, control functions.

References:

1. Pavlenko, V.S. (2021), «Sutnist kiberbezpeky u teorii informatsiinoho prava», *Pravo ta derzhavne upravlinnia*, No. 2, pp. 28–33.
2. Baranov, O.A. (2014), «Pro tlumachennia ta vyznachenni poniattia“kiberbezpeka”», *Pravova informatyka*, No. 2 (42), pp. 54–62.
3. Melnyk, S.V., Tykhomyrov, O.O. and Lienkov, O.S. (2011), «Do problemy formuvannia poniatiĭno-terminolohichnoho aparatu kiberbezpeky», *Aktualni problemy upravlinnia informatsiinoi bezpekoiu derzhavy*, zb. mater. nauk.-prakt. konf., 22 bereznia, NA SB Ukrainy, Kyiv, Vol. 2, pp. 43–48.
4. Furashev, V.M. (2012), «Kiberprostir ta informatsiinyi prostir, kiberbezpeka ta informatsiina bezpeka: sutnist, vyznachennia, vidminnosti», *Informatsiia i pravo*, No. 2, pp. 162–169.
5. Shelomentsev, V.P. (2012), «Pravove zabezpechennia systemy kibernetychnoi bezpeky Ukraïny ta osnovni napriamy ii udoskonalennia», *Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka)*, No. 1 (27), pp. 312–320.
6. Verkhovna Rada Ukrainy (1996), *Konstytutsiia Ukrainy*, document № 254k/96-VR, redaktsiia vid 01.01.2020, pidstava – 27-IX, [Online], available at: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
7. Verkhovna Rada Ukrainy (2018), *Pro natsionalnu bezpeku Ukrainy*, Zakon Ukrainy vid 21.06.2018 r. No. 2469-VIII, [Online], available at: https://zakon.rada.gov.ua/laws/show/2469-19#Text
8. Verkhovna Rada Ukrainy (2010), *Pro rehlament Verkhovnoi Rady Ukrainy*, Zakon Ukrainy vid 10.02.10 r. No. 1861-VI, [Online], available at: https://zakon.rada.gov.ua/laws/show/1861-17/ed20100210
9. Verkhovna Rada Ukrainy (1998), *Pro Radu natsionalnoi bezpeky i oborony Ukrainy*, Zakon Ukrainy vid 05.03.98 r. No.183/98, [Online], available at: https://zakon.rada.gov.ua/laws/show/183/98-вр#Text
10. Verkhovna Rada Ukrainy (2014), *Pro Kabinet Ministriv Ukrainy*, Zakon Ukrainy vid 27.02.14 r. No. 794-VII, [Online], available at: https://zakon.rada.gov.ua/laws/show/794-18#Text
11. Verkhovna Rada Ukrainy (2006), *Pro Derzhavnu sluzhbu spetsialnoho zviazku ta zakhystu informatsii Ukrainy*, Zakon Ukrainy vid 23.02.2006 r. No. 3475-IV, [Online], available at: https://zakon.rada.gov.ua/laws/show/3475-15#Text
12. Verkhovna Rada Ukrainy (2015), *Pro Natsionalnu politsiiu Ukrainy*, Zakon Ukrainy vid 02.07.2015 r. No. 580-VIII, [Online], available at: https://zakon.rada.gov.ua/laws/show/580-19#Text
13. Verkhovna Rada Ukrainy (1992), *Pro Sluzhbu bezpeky Ukrainy*, Zakon Ukrainy vid 25.03.1992 r. No. 2229-XII, [Online], available at: https://zakon.rada.gov.ua/laws/show/2229-12#Text
14. Verkhovna Rada Ukrainy (2015), *Pro Derzhavne biuro rozsliduvan*, Zakon Ukrainy vid 12.11.2015 r. No 794-VIII, [Online], available at: https://zakon.rada.gov.ua/laws/show/794-19#Text
15. Kabinet Ministriv Ukrainy (2015), *Pro zatverdzhennia polozhennia «Pro Ministerstvo vnutrishnikh sprav Ukrainy»*, Postanova vid 28.10.2015 r. No. 878, [Online], available at: https://zakon.rada.gov.ua/laws/show/878-2015-п#Text
16. Kabinet Ministriv Ukrainy (2015), *Pytannia diialnosti Ministerstva informatsiinoi politky Ukrainy*, Postanova vid 14.01.2015 r. No. 2, [Online], available at: https://zakon.rada.gov.ua/laws/show/2-2015-п#Text