Public Policy and Accounting
ISSN 2707-9325

UDC 343.3

Transformation of the administrative and legal status of cybercrime countermeasures entities

Korzun Svitlana[1]

[1] *Postgraduate student*
Zhytomyr State Polytechnic University

Abstract

Cybercrime is becoming increasingly widespread and complex, causing significant harm to both individual citizens and national security. This requires constant improvement of countermeasure mechanisms. The formation and development of a new configuration of state bodies responsible for countering cybercrime is crucial for the effective definition of state criminal policy in this area.

The subject structure of the state policy to counter cybercrime is defined as follows: central executive bodies that implement the state criminal law policy to counter cybercrime; law enforcement entities that are entrusted with the functions of countering cybercrime that are directly related to countering cybercrime; law enforcement entities that are entrusted with the functions of countering cybercrime that are indirectly related to countering cybercrime. To determine the role of subjects of state policy to combat cybercrime in the implementation of the policy under study, the article analyzed regulatory documents regarding their administrative and legal status and powers.

In the process of the study, directions for expanding the tasks and powers of subjects implementing state policy in the following areas were identified: ensuring economic security, financial monitoring, international cooperation in the field of information security; protection of critical infrastructure; law enforcement activities. The author proposed directions for expanding the subject structure of the law enforcement system in combating cybercrime, in terms of creating the National Bureau of Investigation of Cybercrimes and ensuring cyber security, as well as defining its tasks and powers, and formed directions for interaction with other subjects implementing the law enforcement function.

Keywords: state criminal policy; cybercrime; counteraction to cybercrime; subjects of counteraction to cybercrime.

Relevance of the Topic. A defining element in the formation of state criminal policy for combating cybercrime is the transformation of the subject structure of state governance. Currently, there is a lack of institutional support for counteracting cybercrime, as this area is handled solely by the Cyber Police Department under the National Police of Ukraine, which possesses limited functions. Consequently, there is a growing scientific need to establish the administrative and legal status of state governance entities that implement state criminal-legal policy against cybercrime, as well as to expand the subject structure involved in these efforts.

Analysis of Recent Research. These issues have been partially addressed in the scientific works of both domestic and foreign scholars, including T.V. Baranovska, M.O. Budakov, O.M. Budonova, V.M. Butuzov, M.M. Galambo, D.O. Hrytsyshen, A.P. Dykyi, M.O. Dunchykov, V.V. Yevdokymov, N.A. Zahrebelna, I.D. Kazanchuk, R.A. Kalyuzhnyi, N.V. Kaminska, I.V. Karykh, K.O. Kysla, V.V. Kovalenko, Ya.Yu. Kondratiev, B.A. Kormychev, A.V. Kotelevets, O.V. Kravchuk, V.O. Kuchmenko, Yu.Ye. Maksymenko, K.V. Malyshev, A.I. Marushchak, H.V. Novytskyi, T.M. Pushkaryova, S.O. Savchuk, T.S. Yarovyi, T.P. Yatsyk, and others.

Presentation of the Main Material. The subject structure of the state policy for counteracting cybercrime is defined as follows: Central executive authorities responsible for implementing the state criminal-legal policy against cybercrime, namely:

Corresponding author:

[1] ORCID: https://orcid.org/0000-0002-8360-6766

doi: https://doi.org/10.26642/ppa-2024-2(10)-53-62

the Ministry of Digital Transformation of Ukraine, the Ministry of Internal Affairs of Ukraine, the Ministry of Defense of Ukraine, the Ministry of Justice of Ukraine, the Ministry of Finance of Ukraine, the Administration of the State Service for Special Communications and Information Protection of Ukraine, the National Agency of Ukraine for the Detection, Investigation and Management of Assets Derived from Corruption and Other Crimes, the National Agency on Corruption Prevention, and the State Financial Monitoring Service of Ukraine; Law enforcement entities entrusted with functions directly related to counteracting cybercrime, including: the Security Service of Ukraine, the National Police of Ukraine, the State Bureau of Investigations, and the Foreign Intelligence Service of Ukraine; Law enforcement entities entrusted with functions indirectly related to counteracting cybercrime, such as: the National Anti-Corruption Bureau of Ukraine, the Bureau of Economic Security of Ukraine, the State Border Guard Service of Ukraine, the National Guard of Ukraine, the State Customs Service of Ukraine, and the State Protection Directorate of Ukraine.

In order to define their role in the implementation of the studied policy, a legal analysis of normative documents regarding their administrative and legal status and powers has been conducted.

The *Ministry of Digital Transformation of Ukraine*, in accordance with [7], performs the following tasks:

– ensures the formation and implementation of state policy in the following areas: digitalization, digital development, digital economy, digital innovations and technologies, robotics and robotization, e-governance and e-democracy, development of the information society; the introduction of electronic document management; development of digital skills and digital rights of citizens; open data, public electronic registries, development of national electronic information resources and interoperability; electronic communications and the radio frequency spectrum; development of broadband Internet access infrastructure; e-commerce and e-business; provision of electronic and administrative services; electronic identification and trust services, as well as investment in the IT industry; and overall development of the IT industry;

– participates in shaping state policy in the areas of cryptographic and technical information protection, cybersecurity, special-purpose postal services, government courier services, protection of state information resources and information with legally defined protection requirements in information, electronic communication, and information-communication systems, and at information activity facilities; as well as the use of state information resources in terms of information protection, countering technical intelligence, and ensuring the functioning, security, and development of the state government communication system and the National Confidential Communication System;

– participates in the development of virtual assets, blockchain technology, tokenization, and artificial intelligence;

– participates in the development of norms and standards in the fields of electronic identification and trust services, including ensuring interoperability and technological neutrality of technical solutions, and preventing their discrimination;

– participates in developing criteria and procedures for assessing the security state of government information resources in information and communication systems, organizing and conducting such assessments, and providing appropriate recommendations;

– participates in the development and approval of the draft procedure for using the radio frequency spectrum in Ukraine during special periods, under states of emergency or martial law, and in the procedure for the use of the radio frequency spectrum in Ukraine by diplomatic missions, consular posts of foreign states, representations of international organizations in Ukraine, and military formations of foreign states temporarily located on the territory of Ukraine.

This highlights that the *Ministry of Digital Transformation of Ukraine* is a governance entity that regulates and manages the country's virtual space and defines the specificities of implementing and applying modern information technologies.

The *Ministry of Internal Affairs of Ukraine*, based on [3], carries out its activities according to the following components that define the directions of the state criminal-legal policy in counteracting cybercrime:

– develops draft laws and other normative legal acts on matters within its competence;

– reviews and approves draft laws and other legislative acts submitted for approval by other ministries and central executive authorities, and prepares conclusions and proposals regarding draft laws and other legislative acts submitted to the Cabinet of Ministers of Ukraine and the draft laws submitted to the Verkhovna Rada of Ukraine by other entities with the right of legislative initiative, as well as normative legal acts of the Verkhovna Rada of the Autonomous Republic of Crimea;

– develops state programs concerning the assurance of public safety and order, crime prevention, road traffic safety, protection of the state border, protection of objects and territories in case of emergencies, as well as issues related to migration;

– ensures international cooperation, participates in the drafting and conclusion of international treaties of Ukraine on matters within its competence, and ensures the implementation of Ukraine’s international treaties within the limits of its authority as defined by law;

– ensures the functioning of criminal forensic records and records of instruments of criminal offenses and other relevant objects;

– ensures the proper functioning of the unified information system of the Ministry of Internal Affairs, forms and maintains information resources included in the unified information system, processes personal data within the limits of its legal authority, ensures information access regimes, provides informational and qualified electronic trust services, and implements powers regarding digital development;

– conducts informational interaction with other state bodies, law enforcement agencies of foreign states, and international organizations;

– organizes and ensures the operation, development, coordination, and functioning of the Ministry of Internal Affairs’ communication system, manages and monitors the unified departmental digital communication network and the assigned radio frequency spectrum;

– performs the functions of a special user body of the radio frequency spectrum;

– ensures, within its legally defined powers, the protection of information owned by the state or information with restricted access that must be protected according to the law.

Accordingly, the Ministry of Internal Affairs is entrusted with a complex set of tasks aimed at the formation of legal, informational, technical, technological, forensic, and criminological support for the functioning of the law enforcement system as a whole, and of state information security in particular. In addition, an important task of the Ministry is the implementation of the international legal mechanism for combating crime in general.

The Ministry of Foreign Affairs of Ukraine [4] holds the following powers, which define its role and significance in the implementation of state policy:

– ensures the maintenance of diplomatic and consular relations with foreign states, and represents Ukraine in international organizations and special missions;

– safeguards Ukraine's national interests and international security through the promotion of peaceful and mutually beneficial cooperation with foreign states and international organizations, based on universally recognized principles and norms of international law;

– submits proposals regarding the recognition of foreign states by Ukraine and the establishment of diplomatic relations with them;

– ensures the provision of information to the President of Ukraine, the Verkhovna Rada of Ukraine, the Cabinet of Ministers of Ukraine, and other state bodies on major and resonant world events, submits proposals for responses to events directly affecting national interests, and provides information necessary for the implementation of effective foreign and domestic policies;

– submits proposals concerning international initiatives and undertakes measures aimed at enhancing Ukraine's cooperation with foreign states and international organizations;

– disseminates information abroad about Ukraine, its role and place in the world, in order to strengthen the positive international image of the state, and supplies Ukrainian diplomatic missions abroad with relevant informational materials;

– ensures, within the limits of its legally defined authority, the implementation of state policy in the fields of European integration and Euro-Atlantic cooperation;

– ensures the activities of the Commission on Ukraine's Partnership with the North Atlantic Treaty Organization (NATO) and coordinates the development of the Annual National Cooperation Program between Ukraine and NATO;

– protects the rights and interests of Ukraine during the resolution of international disputes involving Ukraine and other subjects of international law;

– ensures the protection of state secrets within the system of the diplomatic service while conducting foreign relations.

In accordance with the above, the Ministry of Foreign Affairs is tasked with ensuring the information security of Ukrainian representations abroad, as well as fulfilling a set of tasks aimed at implementing international legal mechanisms, particularly regarding European and Euro-Atlantic integration and the ratification of international legal instruments.

The Ministry of Defense of Ukraine, in accordance with [5], is endowed with a range of powers that can be attributed to the implementation of the state criminal law policy on combating cybercrime:

– conducts intelligence and information-analytical activities in the interests of national security and state defense;

– coordinates the creation and development of an effective system of strategic communications within the Ministry of Defense and the Armed Forces as part of the national system of strategic communications, ensuring its resilience and adaptability in responding to challenges and threats;

– participates in the implementation of state information policy in the field of defense, in information activities aimed at enhancing the state's defense capabilities and countering the aggressor's (enemy's) information operations, and during martial law coordinates the defense forces in ensuring the formation and implementation of state information policy in the field of defense;

– continuously monitors the information environment, identifies potential and actual information threats in the defense sector, and undertakes appropriate measures;

– ensures the implementation and development of advanced information technologies in the field of defense;

– within its competence, ensures electronic information interaction with government authorities during information exchange to carry out powers defined by law;

– in accordance with established procedures, develops and approves targeted security profiles for information, electronic communication, and information-communication systems owned by the Armed Forces.

The Ministry of Defense of Ukraine is the main entity of state governance that ensures national security and defense of the state, including information security, as well as cyber protection of the state's defense entities.

The Ministry of Justice of Ukraine, in accordance with provision [7], carries out its activities related to combating cybercrime, in particular:

– develops draft laws and other regulatory legal acts;

– prepares proposals for improving legislation and submits them in accordance with the established procedure to the Cabinet of Ministers of Ukraine;

– provides scientific-methodological and organizational-administrative support for the activities of forensic experts who are not employees of state specialized institutions; determines the procedure for exercising control over compliance with legislation regarding forensic activities by forensic experts who are not employees of state specialized institutions, and exercises such control;

– organizes scientific and methodological support for forensic expert activities and carries out organizational and managerial functions concerning the activities of research institutions of forensic expertise under the Ministry of Justice; determines the procedure for monitoring compliance with legislation on forensic expert activities by the research institutions of forensic expertise of the Ministry of Justice and exercises such control;

– prepares proposals for concluding international treaties of Ukraine on issues of international legal relations and legal cooperation in civil and criminal matters, in the field of private international law, and human rights protection;

– engages in international cooperation in the field of enforcement of judgments, establishes and maintains relations with international organizations;

– inspects the implementation by government bodies of obligations undertaken under international treaties of Ukraine concerning international legal relations and legal cooperation in civil and criminal matters, provides recommendations for improving the relevant work, proposes measures to eliminate identified violations and shortcomings, and holds officials accountable for committed violations;

– participates, in accordance with established procedures, in the work of bilateral and multilateral commissions, as well as other international bodies and institutions, approves candidates from Ukraine for membership and staff in international judicial bodies and legal advisers in Ukraine's foreign diplomatic missions;

– within the powers provided by law, participates in the activities of international organizations of which Ukraine is a member and takes measures to fulfill obligations arising from Ukraine's membership in these organizations.

The studied provision does not contain specific tasks aimed directly at combating cybercrime. However, the aforementioned points characterize the Ministry's activities in terms of forming and expert evaluation of the legal framework for the functioning of virtual space and the use of information-computer technologies. Additionally, the Ministry defines the specifics of implementing the criminal law mechanism to combat cybercrime, particularly in the areas of legal, criminological, and forensic support. The Ministry's role is also significant in the implementation of international legal mechanisms through participation in international organizations and the ratification of international treaties.

The Ministry of Finance of Ukraine carries out its activities in accordance with provision [6], which allows identifying the following components related to the implementation of the economic mechanism of the state's criminal law policy on combating cybercrime and its information protection:

– ensures the exercise of powers as the principal budget funds manager in institutions and organizations under the Ministry of Finance's management, as well as in central executive authorities whose activities are coordinated and directed by the Cabinet of Ministers of Ukraine through the Minister of Finance;

– assesses the compliance of budget requests, budget program passports, and draft consolidated cost estimates with budget legislation for the purpose of compiling the state budget;

– analyzes budget requests submitted by the principal budget funds manager to determine their compliance with the Budget Declaration and the efficiency of budgetary fund usage;

– ensures the processing and protection of personal data during verification and monitoring of state payments, and during the verification of the authenticity of information and documents entered into the electronic health care system (except for information on a person's health status). These data form the basis for reports that justify the payment for provided medical services, medicines, and medical devices under the medical guarantees program, or contain personal data of patients and medical workers who provided or received the respective medical services, medicines, and medical devices.

The National Agency of Ukraine for the Detection, Investigation, and Management of Assets Derived from Corruption and Other Crimes operates with the goal of detecting and tracing assets, including those obtained as a result of cybercrimes, as well as identifying assets in the virtual environment. According to provision [9], the following tasks are specified:

– detecting and tracing assets that may be subject to arrest in criminal proceedings or in cases concerning the recognition of assets as unjustified and their recovery to the state budget;

– managing assets that have been seized in criminal proceedings or in cases concerning the recognition of assets as unjustified and their recovery to the state, or that have been confiscated in criminal proceedings or recovered to the state budget following a court decision recognizing them as unjustified;

– managing assets that have been seized or are subject to recovery to the state budget in civil proceedings in cases concerning the recognition of assets as unjustified and their recovery to the state;

– engaging in international cooperation in the field of asset detection, investigation, and management;

– participating in ensuring the representation of the rights and interests of Ukraine in foreign jurisdictions in cases related to the return to Ukraine of assets obtained from corruption and other criminal offenses.

The Agency's activities are particularly significant in terms of countering cybercrime, especially its financial consequences.

The National Agency on Corruption Prevention operates in the following areas:

– analyzes the corruption situation in Ukraine and develops the corresponding Anti-Corruption Strategy and state program for its implementation, as well as coordinates the execution of these documents;

– identifies corrupt norms in legislation and draft legal acts;

– monitors compliance with ethical conduct rules and legislation on conflict of interest prevention in the activities of public officials;

– coordinates and provides methodological assistance to state authorities and local governments in identifying and eliminating corruption risks in their activities, approves and monitors the implementation of anti-corruption programs in these bodies;

– monitors and verifies public officials' declarations, and conducts lifestyle monitoring;

– ensures compliance with restrictions on political party financing, monitors the legal and targeted use of public budget funds by parties, checks the timeliness of their reporting and the accuracy of the submitted information, and distributes state budget funds allocated for the statutory activities of political parties [12].

The issue of corruption prevention is extremely important in the context of new methods of committing corruption offenses through the introduction of information-computer technologies and systems, as well as the increasing human activity in virtual space. Accordingly, the agency is considered an entity involved in the detection of cybercrimes.

The State Financial Monitoring Service of Ukraine «is the central executive authority whose activities are directed and coordinated by the Cabinet of Ministers of Ukraine through the Minister of Finance and which implements state policy in the field of prevention and counteraction to the legalization (laundering) of proceeds obtained through crime, financing of terrorism, and financing of the proliferation of weapons of mass destruction» [2]. The Service's activities are particularly important for financial operations in the virtual environment and the use of information and computer technologies.

The Administration of the State Service of Special Communications and Information Protection of Ukraine «is a central executive authority with a special status, whose activities are directed and coordinated by the Cabinet of Ministers of Ukraine and which ensures the development and implementation of state policy in the areas of special communications, information protection, cybersecurity, and active counteraction to aggression in cyberspace» [1]. This service is classified as a law enforcement entity responsible for combating cybercrime, with functions directly related to cybersecurity. The following tasks are assigned to the agency:

– In terms of regulatory and legal support:

a) ensures regulatory and legal governance in the fields of cryptographic and technical information protection, organization of special communications, government courier services, protection of state information resources and information subject to legal protection requirements in cyberspace, in information and communication systems, and at information activity facilities, counteraction to technical intelligence activities, cybersecurity of critical information infrastructure objects;

b) monitors compliance with information protection legislation in the premises of government communications subscribers;

c) establishes the procedure for organizing and conducting state expertise in the field of cryptographic and technical information protection, conducts state expertise and expert research in the field of cryptographic information protection, defines recommended cryptographic algorithms, authorizes for use cryptographic information protection tools, special communication means, complexes and systems, provides and/or registers expert conclusions based on the results of state expertise in the field of cryptographic and technical information protection, certificates of admission for use of cryptographic information protection tools, means, complexes and systems of special communications, declarations and compliance certificates of comprehensive information protection systems.

– In terms of international activities:

a) participates in the preparation of international treaties of Ukraine on issues within the competence of the State Special Communications Service, prepares proposals for the conclusion and denunciation of such treaties and ensures their implementation;

b) engages in international cooperation, develops proposals for concluding relevant international treaties of Ukraine, and interacts, in accordance with Ukraine’s international agreements, with international organizations on matters within the State Special Communications Service’s competence.

– In terms of technical and technological support:

a) carries out technical regulation in the fields of cryptographic and technical information protection, cybersecurity of critical infrastructure objects, counteraction to technical intelligence activities, protection of state information resources and legally protected information in information and communication systems and information activity objects; organizes, coordinates, and conducts conformity assessment work and develops technical regulations in accordance with established procedures;

b) organizes government communications support for the President of Ukraine, the Chairman of the Verkhovna Rada of Ukraine, the Prime Minister of Ukraine, other officials of state authorities, local self-government bodies, military command bodies, and heads of enterprises, institutions, and organizations during peacetime, emergencies, and special periods;

c) establishes procedures for the creation and admission to operation, and authorizes the use of cryptographic protection means for official information and information constituting a state secret, means, complexes, and systems of special communications; defines cryptographic algorithms for use in information protection tools;

d) organizes the implementation of comprehensive information protection systems at information activity objects and in information and communication systems;

e) establishes procedures and requirements for technical information protection at information activity facilities, for the creation and certification of technical information protection systems, and registers the certification acts of such systems.

– In terms of organizational and methodological support:

a) provides methodological guidance and coordination for the activities of government authorities, local self-government bodies, military formations established under Ukrainian law, and enterprises, institutions, and organizations regardless of ownership, in the areas of cryptographic and technical information protection, counteraction to technical intelligence, as well as in matters related to the prevention of information security violations in information and communication systems, identification and elimination of the consequences of other unauthorized actions against state information resources and legally protected information within information and communication systems;

b) establishes the procedure for state control and carries out such control.

The State Service of Special Communications and Information Protection of Ukraine is a specialized entity for ensuring information security and cybersecurity. It essentially develops security mechanisms for the functioning of virtual space and the use of information-computer technologies and systems within the activities of public authorities. While no specific tasks directly related to combating cybercrime are assigned, this body holds special status and may conduct monitoring activities to counter cyberattacks and cybercrimes.

Security Service of Ukraine (SBU):

«The Security Service of Ukraine, within the limits of its competence as defined by law, is tasked with protecting state sovereignty, the constitutional order, territorial integrity, scientific, technical, and defense potential of Ukraine, the lawful interests of the state, and the rights of citizens from intelligence and subversive activities by foreign special services, encroachments by certain organizations, groups, and individuals, as well as ensuring the protection of state secrets. The Service is also responsible for preventing, detecting, stopping, and solving criminal offenses against peace and humanity, terrorism, and other unlawful acts that directly threaten Ukraine's vital interests» [15].

Currently, a key task of the SBU is ensuring information security and cybersecurity, as well as countering hybrid threats, cyberterrorism, cybercrime, and other virtual space and national security threats that involve information-computer technologies.

National Police of Ukraine:

The National Police is the key law enforcement body engaged in countering cybercrime. According to legislation, it is authorized to:

«counter criminal encroachments on critical infrastructure objects that threaten the safety of citizens and disrupt the functioning of life-support systems; protect critical infrastructure, the interests of society and the state from criminal encroachments in cyberspace; and carry out measures to prevent, detect, stop, and solve cybercrimes targeting critical infrastructure» [14].

The State Bureau of Investigation, in accordance with the legislation [11], performs the following tasks:

– investigation of crimes committed by public officials holding particularly responsible positions as defined in part one of Article 9 of the Law of Ukraine "On Civil Service," individuals whose positions fall under categories one to three of civil service positions, judges, and law enforcement officers, except in cases where such crimes fall under the jurisdiction of the detectives of the National Anti-Corruption Bureau of Ukraine;

– investigation of crimes committed by officials of the National Anti-Corruption Bureau of Ukraine, the Deputy Prosecutor General – Head of the Specialized Anti-Corruption Prosecutor's Office, or other prosecutors of the Specialized Anti-Corruption Prosecutor's Office, except when such crimes are investigated by detectives of the internal control unit of the National Anti-Corruption Bureau of Ukraine;

– investigation of crimes against the established military service procedure (military crimes), excluding those under Article 422 of the Criminal Code of Ukraine.

These crimes may be committed in virtual space or through the use of information-computer technologies, which qualifies them as cybercrime.

The following law enforcement entities are indirectly involved in combating cybercrime:

– *The National Anti-Corruption Bureau of Ukraine* «is a central executive body with a special status, responsible for preventing, detecting, stopping, investigating, and solving corruption and other criminal offenses within its jurisdiction, as well as for preventing new offenses. The Bureau's task is to counteract corruption and other criminal offenses committed by high-ranking officials authorized to perform state or local government functions that pose a threat to national security, and to take other legally prescribed anti-corruption measures» [13]. It should be noted that in the context of the development of the information society, anti-corruption efforts must also be carried out in virtual space, taking into account the use of information-computer technologies by corrupt actors.

– *The Bureau of Economic Security of Ukraine* «is a central executive body tasked with counteracting offenses that threaten the functioning of the state's economy. In accordance with its responsibilities, the Bureau of Economic Security of Ukraine performs law enforcement, analytical, economic, informational, and other functions» [10]. Special attention today must be paid to the issues of cryptoassets and cryptocurrency.

Thus, when studying the legal regulation of the activities of entities implementing state criminal law policy and their administrative-legal status, it is necessary to emphasize the lack of coordinated work in combating cybercrime across various areas of public administration, which requires a transformation of the composition of responsible entities. Our vision of this issue is presented in Table 1.

Table 1
Transformation of the Activities of Entities Implementing the State Criminal Law Policy on Combating Cybercrime

CENTRAL EXECUTIVE AUTHORITIES IMPLEMENTING THE STATE CRIMINAL LAW POLICY ON COMBATING CYBERCRIME			
issues of economic security development			
Ministry of Digital Transformation of Ukraine	**Ministry of Justice of Ukraine**	**Ministry of Finance of Ukraine**	**National Agency on Corruption Prevention**
to assign tasks and expand powers			
– to regulate the issues of production, exchange, circulation, and purchase and sale of crypto assets and cryptocurrency	– to regulate accounting methods for the production, exchange, circulation, and purchase and sale of crypto assets and cryptocurrency		– to regulate the declaration of crypto assets and cryptocurrency by individuals required to submit income declarations;
– to regulate the procedure for the certification and implementation of information technologies and systems in the economic space	– to provide for state programs aimed at increasing public literacy in virtual space and the use of information technologies		– to establish cooperation between entities implementing economic policy regarding the use of information technologies
– to harmonize the issues of protection of information systems related to crypto assets and cryptocurrency	– to harmonize issues related to the formation of reserves in cryptocurrency		– to harmonize issues of insurance in the field of crypto assets and cryptocurrency
issues of asset tracing in financial monitoring			
ARMA [2]	**Ministry of Finance of Ukraine**		**Ministry of Justice of Ukraine**
State Financial Monitoring Service of Ukraine	**National Agency on Corruption Prevention**		**Ministry of Digital Transformation of Ukraine**
to assign tasks and expand powers			
– to regulate the methodologies for investigating the origin of crypto assets and cryptocurrency		– to harmonize the issues of cooperation in tracing monetary, material, and intangible assets in virtual space;	
– to regulate financial monitoring issues concerning crypto assets and cryptocurrency		– to regulate the issues of analyzing suspicious operations in virtual space related to the financing of terrorist activities;	
– to harmonize the issues of creating reserves of monetary, material, and intangible assets in virtual space for operational and investigative activities		– to harmonize the issues of creating reserves of crypto assets and cryptocurrency for operational and investigative activities.	
issues of international cooperation in the field of information security			
Ministry of Foreign Affairs	**Ministry of Justice of Ukraine**	**Ministry of Internal Affairs of Ukraine**	**State Service of Special Communications and Information Protection of Ukraine**
Security Service of Ukraine	**National Police of Ukraine**	**State Bureau of Investigation**	**National Anti-Corruption Bureau of Ukraine**
- to regulate the issues of European and Euro-Atlantic integration of Ukraine's virtual space		- to regulate the use of information-computer technologies and systems in accordance with EU and NATO requirements	
- to regulate integration processes into pan-European cyber-operational and analytical mechanisms such as EU-CyCLONe and CERT-EU		- to regulate the monitoring of compliance with international normative acts ratified by Ukraine	
- to regulate the implementation of the principles of proportionality in all measures related to monitoring and data collection in cyberspace		- to regulate the implementation of EU standards and protocols for the detection, investigation, and prevention of cybercrimes	
- to organize the analysis and continuous monitoring of Ukraine's legislation compliance with EU standards (NIS/NIS2, Europol recommendations, ENISA))		- to develop and monitor the achievement of key performance indicators in ensuring information security and combating cybercrime	

[2] National Agency of Ukraine for Finding, Tracing and Management of Assets Derived from Corruption and Other Crimes

Continuation of Table 1

<table>
<tr><td colspan="4">issues of critical infrastructure protection</td></tr>
<tr><td>Ministry of Defense of Ukraine</td><td>Security Service of Ukraine</td><td>Ministry of Internal Affairs of Ukraine</td><td>Other entities[3]</td></tr>
<tr><td colspan="2">- to regulate the implementation of monitoring and early warning systems (SOC – Security Operations Centers)</td><td colspan="2">- to regulate the issues of operational monitoring of critical infrastructure and key aspects of the virtual environment</td></tr>
<tr><td colspan="4">law enforcement-related issues</td></tr>
<tr><td colspan="4">current structure</td></tr>
<tr><td colspan="2">Ministry of Internal Affairs of Ukraine</td><td>Bureau of Economic Security of Ukraine</td><td>National Anti-Corruption Bureau of Ukraine (NABU)</td></tr>
<tr><td colspan="2">Security Service of Ukraine (SBU)</td><td>National Police of Ukraine</td><td>State Bureau of Investigation (SBI)</td></tr>
<tr><td colspan="2">ARMA (Asset Recovery and Management Agency)</td><td>State Financial Monitoring Service of Ukraine</td><td>State Service of Special Communications and Information Protection of Ukraine</td></tr>
<tr><td colspan="2">- to expand cooperation with INTERPOL and Europol in combating cybercrime</td><td colspan="2">- to establish a unified state information system for investigating cybercrimes</td></tr>
<tr><td colspan="2">- to establish cooperation with entities implementing state policy on the prevention of cybercrime</td><td colspan="2">- to ensure the implementation of EU standards and protocols for the detection, investigation, and prevention of cybercrimes</td></tr>
<tr><td colspan="4">expansion of the institutional structure of the law enforcement system for combating cybercrime</td></tr>
<tr><td colspan="2">Ministry of Internal Affairs of Ukraine</td><td>Bureau of Economic Security of Ukraine</td><td>Національне антикорупційне бюро УкраїниNational Anti-Corruption Bureau of Ukraine (NABU)</td></tr>
<tr><td colspan="2">State Financial Monitoring Service of Ukraine</td><td>National Police of Ukraine</td><td>State Bureau of Investigation (SBI)</td></tr>
<tr><td>Security Service of Ukraine</td><td colspan="2">cooperation with</td><td>ARMA</td></tr>
<tr><td>підпорядкування</td><td colspan="2" rowspan="2">NATIONAL BUREAU FOR CYBERCRIME INVESTIGATION AND CYBERSECURITY ASSURANCE</td><td>accountable to</td></tr>
<tr><td>Cabinet of Ministers of Ukraine</td><td>Verkhovna Rada of Ukraine</td></tr>
<tr><td colspan="4">The National Bureau for Cybercrime Investigation and Cybersecurity Assurance is a state law enforcement agency tasked with the prevention, deterrence, counteraction, detection, suppression, disclosure, and investigation of criminal offenses committed in virtual (cyber) space and other areas involving the use of information and computer technologies, as well as ensuring the cybersecurity of Ukraine.</td></tr>
<tr><td colspan="4">Key tasks:</td></tr>
<tr><td colspan="2">– prevention, deterrence, counteraction, detection, suppression, disclosure, and investigation of criminal offenses involving the production, financing, use, implementation, exchange, and distribution of malicious software (both on physical and non-physical media), components of computer systems used for altering and forging information, intercepting information, interfering with data, gaining unauthorized access to information, generating false information, disseminating illegally obtained information, and other actions prohibited by the criminal legislation of Ukraine.</td><td colspan="2">- prevention, deterrence, counteraction, detection, suppression, disclosure, and investigation of criminal offenses committed using information and computer technologies against individuals, enterprises, government authorities, the state, international organizations, or public administration bodies of other states, which lead to a combination of negative consequences of economic, social, political, infrastructural, and other types, and pose a threat to information, economic, social, food, energy, military, environmental, and political security.</td></tr>
<tr><td colspan="2">– development and implementation of measures to ensure cybersecurity for entities of the legislative, executive, and judicial branches of government.</td><td colspan="2">- development and implementation of measures to counter hybrid threats to the state’s internal and external political security</td></tr>
</table>

[3] Public administration entities implementing state policy in the field of critical infrastructure

Continuation of Table 1

Authorities:	
- to conduct both overt and covert operational-search activities, investigative (search) actions, and covert investigative (search) actions for the purpose of preventing, deterring, countering, detecting, suppressing, disclosing, and investigating criminal offenses committed in the virtual (cyber) space and other areas involving the use of information and computer technologies.	- to have the right to receive free access, in accordance with the procedure established by law, to state information systems and resources, provided such access is justified for conducting overt and covert operational-search activities, investigative and covert investigative actions, in the investigation of uncovered proceedings related to criminal offenses committed in virtual (cyber) space and other spheres involving the use of information and computer technologies.
- to take measures to stop unlawful actions by individuals and legal entities that interfere with the exercise of powers by the National Bureau for Cybercrime Investigation and Cybersecurity Assurance.	- for the purposes of operational-search and investigative activities, creates information systems and maintains operational records within the scope and procedure established by law.
- to engage in cooperation with individuals, including on a contractual basis, while respecting the principles of voluntariness and confidentiality of such relationships; provides material and moral incentives to individuals who assist in the prevention, detection, suppression, and investigation of criminal offenses within the Bureau's jurisdiction.	- to take measures to trace and seize funds and other property that may be subject to confiscation or special confiscation in criminal offenses under the jurisdiction of the National Bureau for Cybercrime Investigation and Cybersecurity Assurance, or that display signs of unjustified acquisition and may be recovered to the state budget. Within the scope of its competence, the Bureau also manages the storage of funds and other property that have been seized.
- to take measures to locate and seize information and computer technologies and systems used in the commission of criminal offenses within the Bureau's competence.	- to engage, within the limits of its competence and on a voluntary basis—including under contractual terms—qualified specialists and experts, including foreign nationals from any institutions, for the purpose of evaluating information and computer technologies and systems.
- to maintain records of criminal cyber offenses.	- to collect and publishes statistical data on cybercrime.

Conclusions. For the effective implementation of the state criminal law policy on combating cybercrime, there is a need for substantial and structural modernization of public administration entities. The directions for expanding the tasks and powers of entities implementing state policy in the areas of economic security, financial monitoring, international cooperation in the field of information security, critical infrastructure protection, and law enforcement activities have been identified. Directions for expanding the institutional structure of the law enforcement system to combat cybercrime have been proposed. In particular, the creation of a National Bureau for Cybercrime Investigation and Cybersecurity Assurance is proposed – a state law enforcement body entrusted with the tasks of preventing, deterring, counteracting, detecting, suppressing, disclosing, and investigating criminal offenses committed in virtual (cyber) space and other areas involving the use of information and computer technologies, as well as ensuring the cybersecurity of Ukraine. The key tasks and powers of this agency have been defined, along with the proposed areas of interaction with other entities performing law enforcement functions. It is proposed that the National Bureau for Cybercrime Investigation and Cybersecurity Assurance be subordinated to the Cabinet of Ministers of Ukraine and report to the Verkhovna Rada of Ukraine.

References:

1. Kabinet Ministriv Ukrainy (2014), *Pro zatverdzhennia Polozhennia pro Administratsiiu Derzhavnoi sluzhby spetsialnoho zviazku ta zakhystu informatsii Ukrainy*, Postanova vid 03 veresnia 2014 r. No. 411, [Online], available at: https://zakon.rada.gov.ua/laws/show/411-2014-%D0%BF#Text
2. Kabinet Ministriv Ukrainy (2015), *Pro zatverdzhennia Polozhennia pro Derzhavnu sluzhbu finansovoho monitorynhu Ukrainy*, Postanova vid 29 lypnia 2015 r. No. 537, [Online], available at: https://zakon.rada.gov.ua/laws/show/537-2015-%D0%BF#Text
3. Kabinet Ministriv Ukrainy (2015), *Pro zatverdzhennia Polozhennia pro Ministerstvo vnutrishnikh sprav Ukrainy*, Postanova vid 28 zhovtnia 2015 r. No. 878, [Online], available at: https://zakon.rada.gov.ua/laws/show/878-2015-%D0%BF#Text
4. Kabinet Ministriv Ukrainy (2016), *Pro zatverdzhennia Polozhennia pro Ministerstvo zakordonnykh sprav Ukrainy*, Postanova vid 30 bereznia 2016 r. No. 281, [Online], available at: https://zakon.rada.gov.ua/laws/show/281-2016-%D0%BF#Text
5. Kabinet Ministriv Ukrainy (2014), *Pro zatverdzhennia Polozhennia pro Ministerstvo oborony Ukrainy*, Postanova vid 26 lystopada 2014 r. No. 671, [Online], available at: https://zakon.rada.gov.ua/laws/show/671-2014-%D0%BF#Text
6. Kabinet Ministriv Ukrainy (2014), *Pro zatverdzhennia Polozhennia pro Ministerstvo finansiv Ukrainy*, Postanova vid 20 serpnia 2014 r. No. 375, [Online], available at: https://zakon.rada.gov.ua/laws/show/375-2014-%D0%BF#Text
7. Kabinet Ministriv Ukrainy (2019), *Polozhennia pro Ministerstvo tsyfrovoi transformatsii Ukrainy*, Postanova vid 18 veresnia 2019 r. No. 856, [Online], available at: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text
8. Kabinet Ministriv Ukrainy (2014), *Pro zatverdzhennia Polozhennia pro Ministerstvo yustytsii Ukrainy*, Postanova vid 02 lypnia 2014 r. No. 228, [Online], available at: https://zakon.rada.gov.ua/laws/show/228-2014-%D0%BF#Text
9. Kabinet Ministriv Ukrainy (2018), *Pro zatverdzhennia Polozhennia pro Natsionalne ahentstvo Ukrainy z pytan vyiavlennia, rozshuku ta upravlinnia aktyvamy, oderzhanymy vid koruptsiinykh ta inshykh zlochyniv*: Postanova vid 11 lypnia 2018 r. No. 613, [Online], available at: https://zakon.rada.gov.ua/laws/show/613-2018-%D0%BF#Text
10. Verkhovna Rada Ukrainy (2021), *Pro Biuro ekonomichnoi bezpeky Ukrainy*, Zakon Ukrainy vid 28.01.2021 r. No. 1150-IX, redaktsiia vid 30.06.2024, pidstava – 3840-IX, [Online], available at: https://zakon.rada.gov.ua/laws/show/1150-20#Text
11. Verkhovna Rada Ukrainy (2021), *Pro Derzhavne biuro rozsliduvan*, Zakon Ukrainy vid 12.11.2015 r. No. 794-VIII, redaktsiia vid 25.10.2024, pidstava – 4009-IX, [Online], available at: https://zakon.rada.gov.ua/laws/show/794-19#Text
12. NAZK, *Pro Natsionalne ahentstvo z pytan zapobihannia koruptsii*, [Online], available at: https://nazk.gov.ua/uk/pro-nazk/
13. Verkhovna Rada Ukrainy (2014), *Pro Natsionalne antykoruptsiine biuro Ukrainy*, Zakon Ukrainy vid 14.10.2014 No. 1698-VII, redaktsiia vid 25.03.2025, pidstava – 4112-IX, [Online], available at: https://zakon.rada.gov.ua/laws/show/1698-18#Text
14. Verkhovna Rada Ukrainy (2015), *Pro Natsionalnu politsiiu*, Zakon Ukrainy vid 02.07.2015 No. 580-VIII, redaktsiia vid 16.08.2024, pidstava – 3528-IX, [Online], available at: https://zakon.rada.gov.ua/laws/show/580-19#Text
15. Verkhovna Rada Ukrainy (1992), *Pro Sluzhbu bezpeky Ukrainy*, Zakon Ukrainy vid 25.03.1992 r. No. 2229-XII, redaktsiia vid 09.01.2025, pidstava – 4156-IX, [Online], available at: https://zakon.rada.gov.ua/laws/show/2229-12#Text