DOI: https://doi.org/10.30525/2256-0742/2025-11-3-267-276

THE ROLE OF OPERATIONAL UNITS OF THE NATIONAL POLICE IN PREVENTING CYBERCRIME IN THE CONTEXT OF ECONOMIC GLOBALISATION AND EXISTENTIAL CHALLENGES

Viacheslav Davydenko[1], Anna Kavunska[2], Viacheslav Barba[3]

Abstract. The *study focuses* on the conceptual, theoretical, empirical and methodological foundations of a legal and economic nature, concerning the legal support for the activities of operational units of the National Police in preventing cybercrime, in the context of economic globalisation and existential challenges. *Methodology.* The present study employed both general and special methods of cognition. Utilising the dialectical method, the author evaluated the essence of countering cybercrime by operational police units in terms of its prevention and prevention of these offences in the legal and economic planes, according to a diverse range of parameters. The analysis established the foundations for a multidimensional study of all the characteristic features of cybercrime prevention in the context of economic integration, in terms of economic and legal etymology. The synthesis established the conditions necessary for the generalisation of the distinctive features of the activities of police operational units. The formal legal method enabled the correct interpretation of the content of legal acts defining the general and special legal regimes of preventive activities of operational police units within the context of economic globalisation and existential challenges. The *purpose of the article* is to provide a comprehensive analysis of the potential areas for improvement in the activities of the operational units of the National Police in order to prevent cybercrime in the context of economic globalisation and existential challenges. The *results of the study* demonstrated that the role of the operational units of the National Police in preventing cybercrime in the context of economic globalisation and existential challenges encompasses a range of complex measures in various areas of activity of the relevant police unit, primarily in ensuring cybersecurity. It has been determined that there are specific areas in which the operational units of the National Police can enhance their efforts to combat cybercrime. These areas have been identified in the context of economic globalisation and existential challenges. *Conclusion.* The advent of cybercrime can be attributed to the prevailing technological transformations in the economy, particularly with regard to the dissemination of information as the primary resource and catalyst for societal advancement. The author's position is that the implementation of economic policies aimed at curbing cybercrime should encompass the following measures: the establishment of a fair and balanced tax system, the formulation of a strategic economic development policy, the promotion of production-oriented initiatives, and the allocation of resources towards the enhancement of public services. From the standpoint of a company's economic security, measures to prevent cybercrime are crucial, due to both local and global economic factors. The analysis of cybercrime legislation enabled the identification of measures of general and special competence taken by the operational units of the National Police. Concurrently, within the legislative framework on national security, which encompasses cybersecurity, the National Police is delineated as a subject of counteraction to such crime, signifying a specialised competence. Concomitantly, the general competence in combating and preventing cybercrime is reflected in the primary function of the National Police, namely to ensure public safety and order, protect human rights and freedoms, the interests of society and the state, and combat crime, including in cyberspace. The primary focus of the implementation of the special competence of operational police units is the Cyber Police

[1] Odesa State University of Internal Affairs, Ukraine *(corresponding author)*
E-mail: davydenkoviacheslav@ukr.net
ORCID: https://orcid.org/0009-0001-4091-3248
[2] Odesa State University of Internal Affairs, Ukraine
E-mail: anuta010588@gmail.com
ORCID: https://orcid.org/0009-0008-1369-4423
[3] Odesa State University of Internal Affairs, Ukraine
E-mail: Barbaslava1@gmail.com
ORCID: https://orcid.org/0000-0001-9436-1699

Department, which is an integral component of the National Police. The Cyber Police Department is responsible for conducting comprehensive operational and investigative activities as a component of the broader strategy to prevent cybercrime. The authors support the view that the following measures, carried out by operational police units, stand out as effective means of countering cybercrime under conditions of existential challenges associated with armed aggression. These measures include counterintelligence, operational and investigative work, and procedural work to counter relevant information threats; the introduction of incentive measures aimed at creating their own information product; the development of their own information and telecommunications infrastructure; and the establishment of communication between civil society and law enforcement agencies in this area.

Keywords: operational units of the National Police, cybercrime, cyberthreat, cybersecurity, shadow economy, economic security, economic globalisation, existential challenges.

JEL Classification: D74, F15, H56, K42

1. Introduction

Recent developments in the study of human societies have revealed a marked tendency towards integration and globalisation across all levels of social organisation, encompassing ethnic groups, nations, states, and regional entities. This phenomenon is consistent with the main features of the formation of the information society, in which information in all its forms and manifestations becomes predominant. This is in accordance with the well-known statement by Nathan Rothschild that "who owns information owns the world".

It is evident that any social processes, in the course of their emergence and development, have the capacity to create both positive and negative imprints on social life. This phenomenon is further compounded by the pervasive dissemination of information and digital products, precipitated by the advent of pertinent technological advancements in specific domains of life. Concurrently, this phenomenon establishes the foundations for the utilisation of such constructions for antisocial, illicit purposes as a tool and means of conducting relevant activities. The aforementioned points are pertinent to the provisions of the UN Convention against Transnational Organized Crime of November 15, 2000 (UNTOC, 2000) and the Council of Europe Convention on Cybercrime of November 23, 2001 (Convention on Cybercrime, 2001). As the first convention also covers cybercrime as a form of transnational organised crime, the second convention includes the following types of criminal offence: offences relating to the confidentiality, integrity and availability of computer data and systems; offences relating to the use of computer facilities; offences relating to the content of data; and offences relating to the infringement of copyright and related rights. It also defines additional types of legal liability and sanctions.

In modern life, cybercrime is one of the most important problems for the development of the state and society. This is particularly true in situations of increased socio-political and socio-economic tension, which are often the result of conflicting interests within geopolitical processes. Such situations can pose an existential threat not only to a particular state, ethnic group or nationality, but also to the world and the world order as a whole. The aforementioned phenomena are exemplified by armed conflicts of a mixed (hybrid) nature, including the armed aggression of the Russian Federation against Ukraine and the civilizational achievements of the European and global community. In such circumstances, it is imperative to address the threat to national interests, encompassing both public and private law dimensions. This necessitates the aggregation of dynamic indicators of cybercrime at both the international and national levels. Concurrently, the repercussions of cybercrime are being felt in numerous facets of national security, including economic security. The correlation between the suppression of socio-economic indicators of state and societal development, and the impact of cybercrime in the banking and financial sectors, is directly proportional, and occasionally in the form of a geometric progression.

Within the overarching structure of the security and defence sector, the National Police, embodied by operational units, constitutes a pivotal entity entrusted with the responsibility of curtailing cybercrime, thereby establishing the foundation for delineating its role in the realm of preventive measures within the paradigm of economic globalisation and existential challenges.

Several researchers have made significant contributions to the study of how cybercrime affects economic indicators of social development. For instance, G.S. Oreku and F.J. Mtenzi (2017) explored the link between cybercrime and the shadow economy, emphasising how one can influence the other. M.S. Dumitrescu and M.E. Marica (2019) examined the rise of cybercrime as a consequence of global economic transformations in the digital era. G.G. Mikhalchenko, Y.M. Snitko, and V.O. Ivanenko

(2023) analysed the broader impact of cybercrime on a nation's economy. A.V. Rosynskyi (2020) focused on how cybercrime affects the digital economy as an integral part of the overall economic structure. Meanwhile, V.A. Golubev (2013) discussed cybercrime as one of the key threats to economic security.

Legal scholars have explored various aspects of the legal nature of cybercrime and the role of the National Police's operational units in its prevention. This research has been conducted within several important contexts, including economic globalisation, existential challenges, and international approaches to combating cybercrime. Notable contributions include: the analysis of global experience in cybercrime prevention (Sayenko, Savela, Topolyansky, 2021); examination of international legal standards in the fight against cybercrime (Popko, Popko, 2021); the study of the powers and responsibilities of the Cyber Police Department within the National Police structure (Bilobrov, 2020); research on combating online child exploitation (Shrago, 2017); the role of law enforcement operational units in cybercrime counteraction (Katerynchuk, 2016); responses to cybercrime amid existential threats (Albul, 2016); and the significance of cyber intelligence in the prevention of cybercrime (Matsaung, Masiloane, 2024).

The aforementioned considerations serve to underscore the necessity for a more comprehensive investigation into the role of operational units within the National Police in the prevention of cybercrime within the context of economic globalisation and existential challenges. This investigation will be the focal point of this article.

2. The Place of Cybercrime in the National and Global Economy

In consideration of the fundamental nature of the economy as a sphere of social existence pertinent to the processes of production, consumption, distribution and exchange of relevant property and non-property benefits of a certain value for an individual or society, it is appropriate to discuss the reproduction of such phenomena in the so-called digital environment. Indeed, a hallmark of the post-industrial information society is the prioritisation of information of various kinds as the primary resource and medium for further development. Indeed, within the information society, the digital environment is becoming predominant among other spheres of circulation of goods of a certain value.

Cybercrime is defined as any unlawful activity that is conducted within the digital environment, with the primary objective of illegally acquiring material benefits or gaining unauthorised access to information and materialised benefits of a significant nature through the utilisation of digital means. The aforementioned points emphasise the universality of cybercrime, on the one hand, as a sphere of illegal activity, and on the other hand, as a means to its implementation.

It is evident that the aforementioned considerations can be fully interpolated to the various processes taking place in the economic sphere, both at the national and international levels.

For instance, statistical evidence demonstrates that cybercrime exerts a multifaceted influence on all sectors of the economy, giving rise to the phenomenon of malicious cyber activity. The magnitude of financial losses resulting from such activities has been estimated to exceed 1 trillion USD over the past decade. This situation directly serves as a prerequisite for the implementation of measures by society to ensure economic security, primarily in countering attacks on mobile technologies, where priority is given to the development of a strategy. The latter should be the product of co-operation between business, government and society to ensure economic growth, foreign investment and security, with the primary focus being on all structural elements of the national and global economy (Tamarkin, 2014).

Concurrently, cybercrime is regarded, in conjunction with corruption and the shadow economy, as a constituent of economic and financial crimes that are concomitant with the level of economic development. The analysis of data concerning economic development and the incidence of this particular crime category within the European Union during the period 2005-2020 yielded the conclusion that the determining factor underpinning this phenomenon is the low level of societal satisfaction. Concurrently, an enhancement in the population's overall well-being fosters the preconditions for an escalation in the level of crime, thereby augmenting the technological dimension of such illicit activities. Within this paradigm, cybercrime occupies a preeminent position. It is evident that a number of economic factors have the capacity to reduce the level of cybercrime. These include fair and balanced tax policy, strategic economic development policy, production development, and investment in public services (Achim, Vaidean, Borlea, Florescu, 2021).

Cybercrime is widely regarded as constituting a pivotal component within the broader ambit of transnational counterfeiting enterprises. According to the researcher, the sphere of cybercrime constitutes a part of the economy in which goods of well-known brands are distributed through illegal activities that utilise the digital environment. These goods are manufactured by completely different entities and are presented as counterfeit goods. The following types of damage caused by the transnational chain conspiracy are highlighted in the above

phenomenon: victimisation by fraud, potential danger to users of counterfeit goods and a negative impact on the legal economy (Albanese, 2019).

A thorough analysis of the nature of cybercrime, in the context of societal and economic developments, reveals that technology, as an agent of change, has a profound impact on all facets of social life. Beyond its capacity to enhance productivity and improve the quality of life for individuals and society at large, the consequences of technological advancement include the transformation of illegal behaviour, with cybercrime representing the pinnacle of this phenomenon. The criminal activity that is perpetrated through the utilisation of various technologies in cyberspace is characterised by the use of computers and computer networks as both the instrument and the location for such illicit activities. The following categories of cybercrime are discussed in the present text: theft, extortion, identity theft, fraud, and corporate espionage. The formation of cybercrime is primarily influenced by technical, social and legal factors. As Oreku and Mtenzi (2017) demonstrate, the role of the shadow economy in the development of cybercrime and their convergence is also determined.

The digital era of human development has given rise to cybercrime, which is associated with the globalisation of this phenomenon, thanks to innovative technological solutions that have made goods and services accessible and verifiable worldwide. In other words, the digitalisation of all economic sectors, coupled with the rationalisation and optimisation of business models, has introduced cybercrime into human life (Dumitrescu, Marica, 2019). In the course of its evolution, cybercrime has given rise to substantial financial flows, which, according to the physical model of an iceberg, exert a deleterious effect on the economic development of society. To prevent this phenomenon, it is proposed that prognostic and strategic steps are taken on a global scale, combining the efforts of countries, peoples, regional entities and corporations to create transparent, competitive business conditions and guarantee a healthy economy. Studying cybercrime in relation to a country's economic development has revealed features such as variability, adaptability and flexibility (Mikhalchenko et al., 2023). The significant impact of this phenomenon on the security component of social life has been noted, especially in the context of the open armed conflict taking place in Ukraine. The 2016 Cybersecurity Strategy of Ukraine (The Decree of the President of Ukraine "On the Decision of the National Security and Defence Council of Ukraine of 27 January 2016 'On the Cybersecurity Strategy of Ukraine'") has been analysed. This has resulted in the prevention of imbalances in the economic indicators of vital societal activity and the creation of an appropriate model for protecting national interests within the framework of cybersecurity and economic security as components of the country's national security. The transformation of a number of processes, coupled with the deepening of existential threats resulting from hybrid aggression against Ukrainian society, has contributed to the development of Ukraine's new 2021 Cybersecurity Strategy (The Decree of the President of Ukraine "On the Decision of the National Security and Defence Council of Ukraine of May 14, 2021 'On the Cybersecurity Strategy of Ukraine'"), which sets out the following strategic goal for ensuring Ukraine's cybersecurity: The creation of secure digital services that strike a balance between the needs of society, the domestic market and the state economy, and the necessary preventive cybersecurity measures. Given the hybrid nature of the aggression against Ukraine, a set of measures, including economic ones, to deter aggressive actions within cyberspace is being considered separately. A significant achievement of Ukraine's 2021 Cybersecurity Strategy is the globalisation of measures to prevent cybercrime, based on respect for human rights, fundamental freedoms, and democratic values, which determine the socio-economic and political development of the state. The strategic development of the national cyberspace as global, open, free, stable and secure is intended to protect state sovereignty and the social and economic development of society. It is therefore appropriate to place the sphere of preventive action against cybercrime within the structure of measures for the country's economic growth.

From a company's perspective, measures to prevent cybercrime are crucial due to local and global economic factors. In this regard, measures are proposed to counteract certain manifestations of cybercrime, particularly those involving social engineering and innovative technological solutions, including software products. These include the following: the recruitment and training of appropriate personnel; the establishment of technologically advanced core resources; and the widespread introduction of digital products with appropriate software support (Rosynskyi, 2020).

In the course of examining the role of cybercrime in the context of economic security, V.A. Golubev has highlighted the necessity of a comparative analysis of economic development indicators and cybercrime levels over a specified period. This analysis should encompass the impact of such illegal behaviour on the Internet and its users, the escalation of cybercrime's proportion within the broader criminal landscape, and the composition and substance of these illegal activities within the economic segments of contemporary nations (Golubev, 2013).

It is reasonable to hypothesise that cybersecurity and cyber defence activities are indeed a component

of the economy, constituting a distinct economic activity that facilitates the transfer of benefits from the material to the digital environment. This approach is substantiated by the finding that a set of cybersecurity measures is effectively categorised as a company expense, thereby exerting a tangible influence on the macro- and microeconomic indicators of a given enterprise (Burov, 2021).

As demonstrated in the analysis of aspects of cybercrime development, the economic and legal foundations for countering cyberthreats have been outlined (Kolesnikov, Ziaylyk, 2017). It is imperative to implement criteria and models for determining qualitative and quantitative indicators of damage caused to the Ukrainian economy as a result of cybercrime, with a view to enhancing the effectiveness of methods of countering cybercrime. This is particularly important in terms of personnel and technological support for computer and technical expertise, and to improve the overall cyber culture of ordinary citizens. In this regard, a number of measures are proposed in the legal, technical, procedural, organisational, resource, and international co-operation areas. Concurrently, enhancing the legal framework to support such initiatives is a priority, and there is a need for comprehensive consensus on this matter.

The logical continuation of the above considerations is the prescriptions of positive law, as exemplified by the provisions of the Law of Ukraine "On Stimulating the Development of the Digital Economy in Ukraine", which directly reproduces measures to create a secure space in the digital environment for the implementation of various economic transactions, mediated, among other things, by the field of cybersecurity and cyber defense (The Law of Ukraine "On Stimulating the Development of the Digital Economy in Ukraine").

Consequently, cybercrime, as a form of illicit activity, occupies a prominent position within the broader framework of the national and global economy. It establishes a system for the unlawful acquisition and redistribution of both tangible and intangible assets, which are reflected within the material and digital domains. The advent of cybercrime can be attributed to the prevailing technological transformations in the economy, particularly with regard to the dissemination of information as the primary resource and catalyst for societal advancement. It is evident that the assertion is substantiated by the existence of economic factors that have the capacity to diminish the prevalence of cybercrime. These factors encompass the implementation of equitable and balanced tax policies, strategic economic development policies, the advancement of production, and the allocation of resources towards the enhancement of public services. In the course of its evolution, cybercrime has given rise to significant financial flows, which, akin to the full-flowing river of the shadow economy, have exerted a destructive impact on the economic development of society. From the standpoint of a company's economic security, measures to prevent cybercrime are crucial, due to both local and global economic factors.

3. The Role of Operational Units of the National Police in Preventing Cybercrime in the Context of Economic Globalisation and Existential Challenges

In light of the preceding examination of cybercrime as a form of illicit conduct within the national and global economy, it is imperative to ascertain the role and functionality of the National Police, embodied by operational units, in the prevention of this egregious phenomenon within the context of global economic integration and the tangible existential challenges pertaining to the threat to national security in terms of its constituent elements. In this paradigm, a particular emphasis is placed on the economic and cybersecurity dimensions of cybercrime, as previously delineated.

In accordance with the United Nations Convention against Transnational Organized Crime of November 15, 2000 (UNTOC, 2000) and the Council of Europe Convention on Cybercrime of November 23, 2001 (Convention on Cybercrime, 2001), the International Criminal Police Organization (INTERPOL) has been assigned a leading role in the development of international co-operation measures to combat cybercrime as a component of transnational crime. This approach is pertinent to the subject matter jurisdiction of criminal offences, which, according to the said normative act, are covered by the content of cybercrime.

The Law of Ukraine "On National Security of Ukraine" explicitly delineates the functional affiliation of the following representatives of the security and defence sector to the subjects of countering cybercrime: the Security Service of Ukraine (Article 19) and the State Service for Special Communications and Information Protection of Ukraine (Article 22) are the relevant authorities in this regard. Moreover, Article 31 of the Law stipulates that the National Coordination Center for Cybersecurity is to be regarded as a working body of the National Security and Defense Council of Ukraine. The aforementioned body is tasked with the coordination and control of the activities of security and defence entities that ensure cybersecurity (The Law of Ukraine “On National Security of Ukraine”). In accordance with the provisions of the Regulation on the National Coordination Center for Cybersecurity, the following entities, which are responsible for the security and defence sectors in the area of cybersecurity, are subject to coordination by this body: the Ministry of Defence, the Armed Forces of Ukraine, the Security Service of Ukraine,

the Foreign Intelligence Service of Ukraine, the Ministry of Foreign Affairs of Ukraine, the Ministry of Digital Transformation of Ukraine, the National Police of Ukraine, the National Bank of Ukraine, the Defence Intelligence of Ukraine, the Intelligence Directorate of the Administration of the State Border Guard Service of Ukraine, and the State Service for Special Communications and Information Protection of Ukraine (The Decree of the President of Ukraine "On National Cybersecurity Coordination Centre").

Article 18 of the Law of Ukraine "On National Security of Ukraine" contains a provision pertaining to the limitation of the powers of the National Police of Ukraine. This includes the powers of the aforementioned institution in the field of combating cybercrime, which are subject to direct regulation in separate legislative acts. The most important of these legislative acts is the Law of Ukraine "On National Police" (The Law of Ukraine "On National Police"). According to clause 24^1 of part 1 of Article 23 of the Law of Ukraine "On National Police", the National Police shall, in accordance with the procedure established by law, counter criminal attacks on critical infrastructure facilities that threaten the safety of citizens and disrupt the functioning of life support systems; protect critical infrastructure facilities, the interests of society and the state from criminal attacks in cyberspace, and take measures to prevent, detect, suppress and solve cybercrime against critical infrastructure facilities. This approach corresponds to a rather narrow understanding of the manifestation of cybercrime in the life of society and individuals. Concurrently, the National Police of General Jurisdiction is tasked with ensuring public safety and order, protecting human rights and freedoms, safeguarding the interests of society and the state, and combating crime. In this regard, the National Police, under the coordination of the Ministry of Internal Affairs of Ukraine in co-operation with other security and defence sector entities, in accordance with Article 27 of the Law of Ukraine "On National Security of Ukraine", participates in the review of public security and civil protection within the comprehensive review of the security and defence sector. This also indirectly includes the determination of the state of counteraction to cybercrime in this manifestation.

The priorities and strategic goals in combating cybercrime, defined by the Cybersecurity Strategy of Ukraine for 2021 (The Decree of the President of Ukraine "On the Decision of the National Security and Defence Council of Ukraine of May 14, 2021 'On the Cybersecurity Strategy of Ukraine'"), fully reflect the subject area of activity of security and defense sector entities, including the National Police. The following activities are therefore identified as priorities: the securing of cyberspace to protect the sovereignty of the state and the development of society; the protection of the rights, freedoms and legitimate interests of Ukrainian citizens in cyberspace; and the integration of Ukraine into the European and Euro-Atlantic cybersecurity field. In order to enhance the capacity to deter various manifestations of cyberthreats, the following objective has been established: the effective counteraction of cybercrime through the acquisition of capabilities by law enforcement agencies, including the National Police, and a state special-purpose body with law enforcement functions, to minimise cybercrime threats, thereby strengthening their technological and human resources to carry out preventive measures and investigate cybercrime. In order to achieve cyber resilience, a number of strategies have been proposed, including professional development, the creation of a society that is digitally literate, and scientific and technical support for cybersecurity. In order to effectively counteract cybercrime, it is proposed to increase the level of knowledge of operational units, pre-trial investigation officers, prosecutors, and judges in the field of information technology and cybersecurity, primarily in the areas of collection and examination of electronic evidence. It is imperative to emphasise the necessity to establish technological capabilities for providers of electronic communication networks and/or services, with the objective of facilitating the integration of technical means for operational search, counterintelligence and intelligence activities.

Moreover, the Action Plan for 2025 for the Implementation of the Cybersecurity Strategy of Ukraine includes the National Police among the subjects for the implementation of 16 tasks (The Decree of the Cabinet of Ministers of Ukraine "On Approval of the Action Plan for 2025 for the Implementation of the Cybersecurity Strategy of Ukraine"), including those that are directly related to the existential challenges that Ukraine has faced due to open armed aggression against it: the introduction of effective mechanisms for interaction between the main subjects of the national cybersecurity system and the defense forces in terms of the joint implementation of cyber defence tasks; development and implementation of the cyber defence plan as an integral part of the defence plan of Ukraine; implementing joint measures with EU and NATO Member States aimed at increasing resilience in cyberspace and the ability to investigate, prosecute cybercrime and respond to cyberthreats; implementing a risk-based approach to measures to ensure cybersecurity of critical infrastructure facilities and state bodies, in particular developing a methodology for identifying and assessing cyber risks at the national level and for critical infrastructure sectors of the state, ensuring regulatory regulation of issues regarding the introduction

of mandatory periodic cyber risk assessments based on the developed methodologies, etc.

A substantial corpus of scientific research has been amassed on the role of the National Police, in particular its operational units, in countering and preventing cybercrime. This research is quite comprehensive in characterising the functionality of such entities. In particular, when analysing cybercrime, which falls directly within the remit of the National Police, the following features are noted: a steady increase in the share of serious crimes, the group nature of their commission, their recurrence, and the dependence of geography on the factor of urbanisation. In order to combat cybercrime, a number of measures have been proposed, including the establishment of reliable operational support for business entities related to the provision of information and telecommunication services. Furthermore, the creation and maintenance of specialised preventive records has been identified as a key strategy, as has the adoption and implementation of the Strategy for Combating Cybercrime of a departmental nature. Additionally, the formation of effective technological support for the protection of computer systems has been recommended, as has the coordination of interagency co-operation in this matter (Kravtsova, 2016).

In light of the findings of the study on international legal standards for combating cybercrime, the following measures are hereby proposed for implementation: comprehensive international co-operation in this domain, mutual assistance and support among countries at the level of interstate contacts, continuous improvement of interstate and national regulations, introduction of international legal standards for criminalising such crimes, and clear regulation of the conceptual and categorical apparatus in this domain. It is proposed that these issues be addressed in the content of a universal convention on combating cybercrime (Popko, 2021).

Drawing upon an analysis of international experience in combating cybercrime, the following measures are proposed to enhance the mechanism for combating cybercrime: the establishment of a mechanism for the rapid restriction or blocking of specific information resources; the introduction of a special legal regime for the search and seizure of electronic evidence; and the establishment of a procedurally significant process for copying information within the framework of the relevant proceedings. Furthermore, there is a need to standardise provisions on the immediate recording and subsequent storage of data by telecommunications operators (providers) and resource (website) owners, ensuring their integrity (Sayenko, Savela, Topolyansky, 2021).

A thorough examination of the competencies of the Cyber Police Department within the overarching National Police structure reveals that its primary functions encompass the implementation of measures aimed at ensuring the state's policy directives within the domain of combating cybercrime. This encompasses the orchestration and execution of operational and investigative functions in strict adherence to legal frameworks, in addition to administrative, regulatory, personnel, information support, preventive, and prophylactic functions. In the context of measures to prevent cybercrime, the following approaches are proposed: firstly, the monitoring of cyberthreats, cyberattacks and cyber incidents; secondly, the provision of information about cybercrime and cybercrimes, and the raising of public awareness about security in cyberspace; thirdly, the development of domestic software and hardware; fourthly, the establishment of coordination and interaction between cybersecurity entities on a partnership basis at both the national and international levels; fifthly, the improvement of the regulatory framework for cybersecurity; and sixthly, the shaping of a culture of online behaviour (Bilobrov, 2020).

In the context of combating child exploitation using the Internet, measures have been identified to combat prohibited content, and effective ways to combat this type of cybercrime have been outlined, including: standardising rules of conduct on the Internet; staffing law enforcement training in this area; strengthening sanctions against offenders; coordinating the efforts of law enforcement agencies at the national and international levels; extending the legal regime of mass media to the Internet; and standardising the conceptual and categorical apparatus in this area (Shrago, 2017).

Among the search activities carried out by operational units, including those involved in combating cybercrime, a special place is given to operational profiling. This is a set of psychological methods and techniques used to assess and predict a person's behaviour by analysing their most informative personal characteristics and personality traits. These traits also tend to manifest in the digital environment as a result of a cybercriminal's behaviour. As a method of combating cybercrime, operational profiling is distinguished by the use of system and network analysis as a means of working with files and data of various kinds. In this regard, amendments to the current legislation are proposed to legalise operational profiling in the system of cyber police powers, as well as to provide professional training for these employees (Zachek, 2020).

In order to address the issue of cybercrime prevention by the operational units of the National Police as part of the countering of such crimes, it is proposed that the entire range of measures within the latter concept be extended to the sphere of prevention, such as prevention, search, development, etc. Furthermore, it is proposed that the terms of operational and investigative prevention and prevention of cybercrime

be intertwined in the context of the aforementioned. In this regard, relevant regulatory innovations in this area are proposed (Gribov, Chernyak, 2018).

A study of the role of law enforcement agencies in combating cybercrime has enabled the following measures for preventing this type of crime to be identified: the creation, certification, licensing, and implementation of the necessary technical and software means of information protection; the creation of specialised organisational structures of administrations and computer security services, whose task is to ensure the reliable functioning of means of protection, generating keys and passwords, distributing them, controlling their use, replacement, and destruction; and training qualified personnel (Katerynchuk, 2016).

In the context of countering cybercrime in the face of existential challenges associated with armed aggression, the following measures are proposed: counterintelligence, operational and investigative, and procedural work to counter relevant information threats; introduction of incentives aimed at creating own information product; development of own information and telecommunications infrastructure; establishment of communication between civil society and law enforcement agencies in this area (Albul, 2016).

A particular function in the prevention of cybercrime is attributed to the employment of cyber intelligence and cybersecurity measures for the purpose of monitoring cyberspace. Concurrently, attention is drawn to the peculiarities of legitimising electronic evidence obtained in analogous cases in the relevant proceedings and the need to regulate this issue (Matsaung, Masiloane, 2024).

A significant aspect of the prevention of cybercrime is the issue of co-operation between operational police units and other police units, such as the municipal security police. This indicates the necessity to coordinate the activities of these units as a guarantee of overall prevention, similar to other types of crime (Kopotun et al., 2020).

A comparative study has been conducted to inform a series of proposed measures to prevent cybercrime. These measures include the coordination and co-operation of all entities involved in combating cybercrime, the formation of an appropriate regulatory framework and specific policies for the work of relevant police units, the development and implementation of technologies for detecting and preventing offences, including the use of operational search methods and innovative technological solutions, and the creation and implementation of relevant training programmes in the professional education system for police officers (Bello, 2018).

Consequently, within the overarching framework of countering cybercrime, measures to prevent this particular type of crime in the context of the role of operational police units in this activity are frequently considered in conjunction with measures to prevent the commission of these offences. The analysis of the legislation on combating cybercrime made it possible to identify measures of general and special competence carried out by the operational units of the National Police. Concurrently, within the legislative framework on national security, which encompasses cybersecurity, the National Police is delineated as a subject of counteraction to such crime, signifying a specialised competence. Concomitantly, the general competence in combating and preventing cybercrime is reflected in the primary function of the National Police, namely to ensure public safety and order, protect human rights and freedoms, the interests of society and the state, and combat crime, including in cyberspace.

4. Conclusions

In summary, the following observations are warranted in consideration of the function of operational units of the National Police in the prevention of cybercrime within the context of economic globalisation and existential challenges.

Cybercrime, as a form of illegal activity, occupies a prominent place in the structure of the national and global economy. It creates a mechanism for the illegal acquisition and redistribution of both property and non-property benefits, which are reflected among the objects of the material and digital world. The advent of cybercrime can be attributed to the prevailing technological transformations in the economy, particularly with regard to the dissemination of information as the primary resource and catalyst for societal advancement. It is stated that the economic levers that reduce cybercrime include fair and balanced tax policy, strategic economic development policy, production development and investment in public services. As it evolves, cybercrime creates significant financial flows within the shadow economy. Like the physical model of an iceberg, this has a destructive impact on the economic development of society. From a company's perspective, measures to prevent cybercrime are crucial due to local and global economic factors.

In the context of countering cybercrime, measures to prevent this type of crime are often considered alongside measures to prevent the commission of these offences, particularly in relation to the role of operational police units in this activity. Analysing the legislation on combating cybercrime revealed measures of general and special competence carried out by operational units of the National Police. At the same time, within the framework of national security legislation, including cybersecurity, the National Police is quite narrowly defined as an entity combating such crimes, which indicates special competence. At the

same time, general competence in combating and preventing cybercrime is reflected in the main task of the National Police, namely: ensuring public safety and order, protecting human rights and freedoms, the interests of society and the state, and combating crime, including in cyberspace.

The primary entity entrusted with the implementation of the special powers of the police operational units is the Cyber Police Department within the National Police. This department, as part of measures to prevent cybercrime, carries out the following functions: monitoring cyberthreats, cyberattacks, and cyber incidents; providing information about cybercrime and cyber incidents and raising public awareness about cybersecurity; developing domestic software and hardware; establishing coordination and interaction between cybersecurity entities on a partnership basis at both the national and international levels; improving the regulatory framework for cybersecurity; and shaping a culture of online behaviour. A significant role is assigned to operational profiling within the framework of systemic and network analysis of relevant volumes of information in the prevention of such crimes in the activities of operational units. It is widely accepted that, in order to combat cybercrime in the context of existential challenges related to armed aggression, operational police units implement a range of measures. These include counterintelligence, operational-investigative, and procedural work to counter relevant information threats; the introduction of incentives aimed at creating their own information product; the development of their own information and telecommunications infrastructure; and the establishment of communication between civil society and law enforcement agencies in this area.

In the context of these measures, proposals are put forward to enhance the organisational and legal support for the operations of police units, with the aim of preventing cybercrime in the era of economic globalisation and existential challenges.

References:

UNTOC (2000). United Nations Convention Against Transnational Organized Crime.

Convention on Cybercrime (2001). Council of Europe conventions on cybercrime.

Oreku, G. S., & Mtenzi, F. J. (2017). Cybercrime: Concerns, Challenges and Opportunities. *Information Fusion for Cyber-Security Analytics,* 691, 129–153.

Dumitrescu, M. S., & Marica, M. E. (2019). Cybercrime in Digital Era. *Basiq International Conference: New Trends in Sustainable Business and Consumption,* pp. 433–440.

Mikhalchenko G. G., Snitko, Y. M., & Ivanenko, V. O. (2023). Cybersecurity in the economy: protection against cyberthreats in the digital world. *Scientific notes of Lviv University of Business and Law. Economic series. Legal series*, 38, 377–384.

Rosinsky, A. V. (2020). Cybercrime as a challenge to the economic security of enterprises in the context of forced digitalization. Economic, managerial, and information-analytical innovations in construction: II International Scientific and Practical Conference. P. 109–111.

Golubev, V. A. (2013). Analysis of cybercrime in the field of economic security. *Information Technology and Security*, 1(3), 26–32.

Sayenko, M. I., Savela, E. A., & Topoliansky, Y. Y. (2021). International experience in combating cybercrime and cyber fraud. *Scientific Bulletin of Uzhhorod National University: Law Series*, 64, 386–391.

Popko, V. V., & Popko, E. V. (2021). International legal regulation of transnational cybercrime in cyberspace. *Scientific Bulletin of Uzhhorod National University: Law Series*, 66, 276–283.

Bilobrov, T. V. (2020). Administrative and legal status of the Cyber Police Department of the National Police of Ukraine. Dissertation/Thesis: National Academy of Internal Affairs (Kyiv).

Shrago, A. O. (2017). International experience in combating the exploitation of children on the Internet and its use in the activities of operational and investigative units of the National Police. *Operational and investigative activity of the National Police: problems of theory and practice*: Materials of the All-Ukrainian Scientific and Practical Conference, pp. 118–122.

Katerynchuk, I. P. (2016). Law enforcement agencies in the fight against cybercrime. *Cybersecurity in Ukraine: legal and organizational issues*: Materials of the All-Ukrainian Scientific and Practical Conference, pp. 4–6.

Albul, S. V. (2016). Countering information threats in the context of the anti-terrorist operation. *Cybersecurity in Ukraine: legal and organizational issues*: Materials of the All-Ukrainian Scientific and Practical Conference, pp. 7–8.

Matsaung, P., & Masiloane, D. T. (2024). The role of cyber intelligence in policing cybercrime in South Africa: Insights from law enforcement officers. *African Security Review*, 34(2), 152–167.

Tamarkin, E. (2014). Cybercrime: a Complex Problem Requiring a Multi-faceted Response: Report. *Institute for Security Studies*.

Achim, M. V., Vaidean, V. L., Borlea, S. N., & Florescu, D. R. (2021). The Impact of the Development of Society on Economic and Financial Crime. Case Study for European Union Member States. *RISKS,* 9(5).

Albanese, J. S. (2019). Cybercrime as an Essential Element in Transnational Counterfeiting Schemes. *Journal of Digital Forensics*, pp. 51–57.

The Decree of the President of Ukraine "On the Decision of the National Security and Defence Council of Ukraine of January 27, 2016 'On the Cybersecurity Strategy of Ukraine'" of March 15, 2016, No. 96/2016. The Official Bulletin of the Verkhovna Rada of Ukraine (BVR). Available at: https://zakon.rada.gov.ua/laws/show/96/2016?lang=en#Text

The Decree of the President of Ukraine "On the Decision of the National Security and Defence Council of Ukraine of May 14, 2021 'On the Cybersecurity Strategy of Ukraine'" of August 26, 2021, No. 447/2021. The Official Bulletin of the Verkhovna Rada of Ukraine (BVR). Available at: https://zakon.rada.gov.ua/laws/show/447/2021?lang=en#Text

Burov, O. (2021). The impact of cybercrime on the digital economy. *Theory and practice of intellectual property*, 5, 69–78.

Kolesnikov, A., & Zyailyk, M. (2017). Economic and legal measures for the development of cybercrime and methods of combating it. *Current Problems of Jurisprudence*, 1(9), 26–29.

The Law of Ukraine "On Stimulating the Development of the Digital Economy in Ukraine" of July 15, 2021, No. 1667-IX. The Official Bulletin of the Verkhovna Rada of Ukraine (BVR). Available at: https://zakon.rada.gov.ua/laws/show/1667-20?lang=en#Text

The Law of Ukraine "On National Security of Ukraine" of June 21, 2018, No. 2469-VIII. The Official Bulletin of the Verkhovna Rada of Ukraine (BVR). Available at: https://zakon.rada.gov.ua/laws/show/2469-19?lang=en#Text

The Decree of the President of Ukraine "On National Cybersecurity Coordination Centre" of June 7, 2016, No. 242/2016. The Official Bulletin of the Verkhovna Rada of Ukraine (BVR). Available at: https://zakon.rada.gov.ua/laws/show/242/2016?lang=en#Text

The Law of Ukraine "On National Police" of July 2, 2015, No. 580-VIII. The Official Bulletin of the Verkhovna Rada of Ukraine (BVR). Available at: https://zakon.rada.gov.ua/laws/show/580-19#Text

The Decree of the Cabinet of Ministers of Ukraine "On Approval of the Action Plan for 2025 for the Implementation of the Cybersecurity Strategy of Ukraine" of March 7, 2025, No. 204-p. The Official Bulletin of the Verkhovna Rada of Ukraine (BVR). Available at: https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text

Kravtsova, M. O. (2016). Cybercrime: Criminological Characterization and Prevention by Internal Affairs. Dissertation/Thesis: Kharkiv National University of Internal Affairs.

Zachek, O. I. (2020). The use of profiling to combat cybercrime. *Socio-legal studies*, 4(10), 94–100.

Hrybov, M. L., & Chernyak, A. M. (2018). Operational units of law enforcement agencies of Ukraine as subjects of combating crime. Operational units of law enforcement agencies of Ukraine as subjects of combating crime. *Journal of Criminal Justice,* 4, 8–17.

Kopotun, I., Nikitin, A., Dombrovan, N., Tulinov, V., & Kyslenko, D. (2020). Expanding the Potential of the Preventive and Law Enforcement Function of the Security Police in Combating Cybercrime in Ukraine and the EU. *Tem Journal-Technology Education Management Informatics,* 9(2), 460–468.

Bello, M. (2018). Investigating cybercriminals in Nigeria : a comparative study. Dissertation/Thesis: University of Salford.

Received on: 13th of June, 2025
Accepted on: 28th of July, 2025
Published on: 13th of August, 2025