UDC 343.533
DOI: 10.63341/naia-herald/4.2025.77

Cybercrime: Analysis of new challenges and legal mechanisms of counteraction

Alina Chukaieva*
Doctor of Philosophy in Law, Associate Professor
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0001-8251-5187

■ **Abstract.** The situation of the spread of hybrid means of warfare contributes to the rapid growth of information crimes of various forms and methods of commission, including those of a complex nature. The purpose of this study was a thorough critical understanding of the main approaches to countering relevant types of cybercrime. The study used systematic, comparative and legal, formal and logical, and functional methods. It was noted that in the national legislation on the legal regulation of the field of cybersecurity, there are a number of gaps that complicate cooperation with other states in countering cybercrime and reduce the effectiveness of security measures, and also suggested ways to eliminate them. The need to streamline the conceptual framework that serves the field of cybersecurity (for example, providing a clear definition of the concept of cyberwarfare), and harmonise national legal norms with relevant international legislation, considering the expediency of unifying the legal norms of different states when regulating the actions of the parties for the effectiveness of international cooperation in combating cybercrime, was emphasised. It was noted that overcoming global cybersecurity problems requires consolidating the efforts of the world's states, improving legal and technical mechanisms, and establishing the foundations of a security culture in cyberspace. The need to create an effective mechanism that would simultaneously guarantee information security of the state and protect democratic rights and freedoms was noted. The practical significance of the results obtained lies in the possibility of using them to improve national legislation in the field of cybersecurity and countering cybercrime, in particular, in the development and adjustment of regulatory legal acts considering the requirements of international law and the provisions of the Budapest Convention

■ **Keywords:** cybersecurity; cyberspace; cyberwarfare; hacker; information; ethical standards; international cooperation

■ Introduction

In times of digital transformation of public relations, computer and information technologies, due to the rapid development and expansion of the use of the Internet, computers, mobile gadgets, and other digital technologies, have become an integral part of human life and at the same time one of the biggest challenges for the national security of countries. Nowadays, rapidly developing, they cover all spheres of life – the economy, critical infrastructure, public administration, social communications, etc., and, accordingly, the risks associated with the misuse of digital resources are growing. Thus, cybercrime is one of the most pressing problems of our time, and its manifestations (cyber-attacks, financial fraud, unauthorised access to information systems, the spread of malicious software, etc.) are

■ **Suggested Citation:**
Chukaieva, A. (2025). Cybercrime: Analysis of new challenges and legal mechanisms of counteraction. *Scientific Journal of the National Academy of Internal Affairs,* 30(4), 77-87. doi: 10.63341/naia-herald/4.2025.77.

■ *Corresponding author

■ Received: 29.06.2025; Revised: 02.10.2025; Accepted: 25.11.2025

a phenomenon that is not inferior in importance and prevalence to classical methods of committing crimes, especially in the context of a full-scale war between Ukraine and the Russian Federation, when cyberspace, like land, sea, air, and space, has really turned into a separate very important field of military operations. The aggressor country resorts to cyber threats using the latest technical means (criminal cyber-attacks, espionage, fraud, etc.) as part of the implementation of hybrid forms of aggression against economic, political, technical, military and information security and sovereignty of Ukraine, aimed at destabilising critical infrastructure and information systems of the country, and therefore, the search for ways to prevent the main types of cybercrime, develop cybersecurity strategies to protect citizens, and continuously improve mechanisms to counteract this type of crime becomes particularly relevant. The emergence of AI, blockchain, and other new digital technologies are forcing cybersecurity professionals around the world to constantly review their methods of combating cybercrime.

Thus, despite the fact that various aspects of the problem of cybercrime have been actively studied for decades, the extreme intensity of changes in this area (in 2025, the very nature of cyber threat risks in the world has changed significantly – in cyberspace, as a huge strategic domain, powerful resources are being created for political and economic dominance, and the priorities of countering risks are gradually shifting towards continuous adaptation to them), the continuous invention of new ways of committing cybercrime by intruders and, accordingly, the need for constant development of effective methods of countering them, the emergence of new trends in understanding this issue in the context of world discourse, they determine the timeliness of scientific research.

Various aspects of the problem of cybercrime and ways to counteract it are constantly in the focus of attention of the global scientific community. Thus, E.H. Spafford *et al.* (2023) argued that society is exposed to significant risks, including threats in energy, communications and transportation systems; privacy violations; data falsification; and new types of theft and fraud have also emerged. However, if earlier the subjects of cybercrime were individual criminals, anarchists, extremists, cyberterrorists, then the modern world is more characterised by terrorist networks that seek to seize the tools of democratic governance (DeMillo & Spafford, 2025).

S.B. Karvatska *et al.* (2025), after studying key data protection, cyber defence, and cyberwarfare issues, noted their simultaneous technological uniqueness and legal certainty. They also stressed the importance of creating a harmonised international legal framework for resolving cybersecurity and data protection issues. R. Shak (2024) spoke about the development of narrow (information security protection) and broad (combating all types of offences committed using information and telecommunications technologies) approaches to understanding the concept of cyber-violation or cybercrime. The narrow approach focuses on protecting information security, while the broad approach covers all types of criminal acts committed using information and communication technologies. The researcher noted that it is necessary to develop a unified approach to the definition of cyber violations and develop legislation in accordance with new challenges in the field of cybersecurity. M.I. Krasko & A.I. Tsevukh (2025) defined cybercrime as a socio-legal phenomenon that has a hybrid nature: it simultaneously functions within technical, economic, legal, and even political systems. The main features of cybercrime are anonymity, dynamism, cross-border nature, and high technology. These characteristics make it impossible for countries to respond effectively alone.

The purpose of this study was to critically examine the main approaches to combating such cybercrimes

Materials and Methods

For this research, a number of principles, approaches, and methods were applied to achieve scientific objectivity and comprehensive coverage of the topic. First of all, it is necessary to note the use of an interdisciplinary (interdisciplinary) approach, since information security issues, which at first glance appear to be purely technical in nature, relate to various scientific fields, primarily legal, social, economic, financial, security, etc., and should be considered in the socio-legal and, to a large extent, political sphere. The study was also characterised by a criminological approach, which helped to analyse the nature of cybercrime, its manifestations, features of the identity of a cybercriminal hacker, mechanisms of occurrence of their criminal behaviour, etc. The research methodology included: a systematic method – to investigate the typology of cybercrime, highlighting the components of the system of response and protection to cyber threats, etc.; comparative legal – to analyse international and national cybersecurity legislation for positive achievements and shortcomings; a formal logical method – to formulate the author's opinion on certain aspects of the study based on the scientific analysis carried out; functional – to determine the subjects of legal regulation of the problem of cybercrime.

To conduct a study of the legal regulation of cybercrime problems, the authors mainly used the experience of the European Union and Ukraine, in particular during the war. During the analysis of

laws and regulations, it was studied and analysed as international legal documents, including the Convention on Cybercrime[1], (Budapest Convention), United Nations Convention Against Cybercrime [2], and Ukrainian: Cybersecurity strategy of Ukraine[3], Criminal Code of Ukraine[4] (section "Crimes in the sphere of use of electronic computers (computers, systems and computer networks and telecommunication networks"), in particular Article 361 "Unauthorised interference in the operation of information (automated), electronic communication, information and communication systems, electronic communication networks", laws of Ukraine "On Amendments to the Criminal Procedure Code of Ukraine and the Law of Ukraine "On Eectronic Communications"[5], Law of Ukraine "On the Main Principles of Ensuring Ukraine's Cybersecurity"[6], etc.

Results and Discussion

Cybercrime is a collection of offences committed using information and telecommunications technologies that encroach on information security and/or use a computer, and other devices that provide access to the network, as a tool or means of committing a crime (Shak, 2024). As of 2025, along with the term "cybercrime" in international and Ukrainian legal science, such concepts as "criminal acts in the field of computer information" and "crimes committed using information technologies" were most often used.

The phenomenon of cybercrime is cross-border in nature. Due to the global and cross-border nature of computer and telecommunications systems and the possibility of identity falsification, situations arise when a person commits an offence from one continent against an object on another, and its results appear on a third (Dulepa, 2021; Dykyi *et al.*, 2025). Events take place in cyberspace, in which T.V. Fedorenko & V.V. Fedorenko (2023) considered two components:

1) information in digital format, which exists in two forms: static (files stored on media) and dynamic (network packets, data streams, commands, and requests that circulate in networks are processed by automated systems and submitted to the user in graphic or text form);

2) technical infrastructure, IT technologies and software tools that provide the main processes of working with information – its collection, processing, storage and transmission: Internet infrastructure and network communications, computer equipment, mobile devices, and other gadgets.

Advanced cyber threats are characterised primarily by their global scale, due to the lack of geographical boundaries on the Internet. Any cyberattack can potentially target information systems and networks located in different countries, which significantly complicates the coordination of international efforts to counter cybercrime. An additional risk factor is the high level of anonymity in the digital environment: attackers often use anonymous networks or fictitious digital identities, which significantly complicates their identification and legal liability.

The problem of attributing cyber-attacks is particularly difficult, since various technical means are used to hide the real source of interference, in particular, IP spoofing, routing traffic through intermediate nodes, or using botnets. As a result, establishment of the initiator of an attack is often a long and resource-intensive process. Moreover, advanced cyber threats are characterised by a high level of innovation: cybercriminals are constantly improving their methods, actively introducing the latest technologies, in particular artificial intelligence, machine learning, and advanced cryptographic solutions. This not only increases the effectiveness of criminal actions, but also significantly complicates the functioning and adaptation of cyber defence systems (Haiduk & Zverev, 2024; Krasko & Tsevukh, 2025).

The main characteristic features of cybercrimes that distinguish them from other threats are spatial boundaries, the possibility of global development in the shortest possible time, the lack of subject binding to specific actions in cyberspace (usually cyber-attacks are carried out by competent persons at the appropriate order of the subjects of confrontation) (Dolzhenko, 2020). There is no clear regulatory framework for classifying cybercrime (Dovzhenko, 2019). In accordance with the Council of Europe Convention on Cybercrime[7], cyber activity of a criminal nature is conventionally divided into four groups: offences against the confidentiality, integrity, and availability of computer data and systems (illegal access, data interception, interference with data and systems, abuse

[1] Convention on Cybercrime. (2001, November). Retrieved from https://www.coe.int/en/web/cybercrime/the-budapest-convention.
[2] United Nations Convention Against Cybercrime. (2024, December). Retrieved from https://zakon.rada.gov.ua/laws/show/3551-12#Text.
[3] Decision of the National Security Council of Ukraine "On the Strategy of Cybersecurity of Ukraine". (2021, August). Retrieved from https://zakon.rada.gov.ua/laws/show/n0055525-21#Text.
[4] Criminal Code of Ukraine. (2001, April). Retrieved from https://kku.com.ua/chastyna-2/rozdil-16/.
[5] Law of Ukraine No. 2137-IX "On Amendments to the Criminal Procedure Code of Ukraine and the Law of Ukraine 'On Electronic Communications' to Enhance the Efficiency of Pre-Trial Investigations "Hot on the Trail" and Counter Cyberattacks". (2022, March). Retrieved from https://zakon.rada.gov.ua/laws/show/2137-20#Text.
[6] Law of Ukraine. No. 2163-VIII. "On the Main Principles of Ensuring Ukraine's Cybersecurity". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text.
[7] Council of Europe Convention on Cybercrime. (2001, November). Retrieved from https://surl.li/fuzlrz.

of devices); computer-dependent crimes (forgery and fraud related to computers); crimes related to content (in particular, crimes related to child pornography); violations of copyright and related rights.

Yu.V. Nedilko (2018) proposed an alternative division into aggressive and non-aggressive cybercrimes. Aggressive ones include cyberterrorism, threats of physical violence (including via email), cyber espionage, cyber stalking, and the creation and distribution of child pornography. Non-aggressive include cyber theft, cyber vandalism, cyber fraud, cyber espionage, distribution of spam and malicious software. The emergence of numerous cyber threats has forced the international community to develop a legal framework for the security of cyberspace. The first international legal act that took measures to unify the list and signs of cyber violations was Convention on Cybercrime[1], which has been ratified by 67 states. In this document, states parties are invited to criminalise encroachments on such objects as information (computer) security, property, intellectual property, and actions related to the distribution of illegal content on information networks (child pornography; information of an extremist nature). A similar interpretation of cybercrime can be traced in other directives such as NIS2[2] and CER[3] countries – parties to the Convention on countering attacks on information networks, and maintaining the security of networks and information systems (Shak, 2024).

The UN and EU documents on cybercrime mention not only "computer" offences that encroach on information security, but also other criminal acts that use a computer as a weapon (computer-facilitated) or a means of offence (computer-related). This opinion seems to be generally correct, since the use of information and telecommunications technologies as a tool or means of criminal encroachment on any objects increases the effectiveness of criminal activity, giving it a qualitatively new form, making it cross-border, large-scale, and difficult to study. However, according to R. Shak (2024), the above-mentioned documents of the UN and the European Union do not say anything about countering the use of information and telecommunications technologies as weapons in military and political conflicts, for interfering in the internal affairs of states, carrying out subversive, terrorist, espionage and sabotage activities, etc. However, national approaches to criminal legislation in the field of countering cybercrime, law enforcement practices, and methods of maintaining criminal statistics differ significantly from country to country. Thus, no criminological analysis can fully cover the global scale of this problem (Dolia, 2024).

Ukrainian legislator defines cybercrime as a socially dangerous act in cyberspace and/or with its use, the responsibility for which is provided for by the law on criminal liability and/or which is recognised as a crime by international treaties of Ukraine[4]. In addition, the concept of "cybercrime" combines criminal offences provided for in Section XVI of the Criminal Code of Ukraine[5] "Crimes in the sphere of use of electronic computers (computers, systems, and computer networks and telecommunication networks", and registered criminal proceedings with a qualifying mark in the card on a criminal offence – "using high information technologies and telecommunications networks". According to Section XVI of the Criminal Code of Ukraine "Crimes in the sphere of use of electronic computers, systems, and computer networks and telecommunication networks", the main types of cybercrime are: unauthorised interference in the operation of computer systems, creation and distribution of malicious software, illegal sale or disclosure of information with restricted access, illegal actions with data on the part of persons who have access to them, violation of the rules of operation or protection of information, and obstruction of networks by mass mailings (articles 361-363-1). In addition to Section XVI of the Criminal Code of Ukraine, cybercrime can also include a number of other offences committed using information technologies. In particular, these are crimes in the field of intellectual property (Article 176, Article 229), illegal actions with bank documents and payment cards (Article 200), fraud and theft (Article 185, Article 190), violation of bank secrecy (Article 231), and offences related to the distribution of pornography (Article 301). Special attention should be paid to crimes committed through social networks and other Internet resources: driving to suicide (Article 120), bribery of voters (Article 160), violation of equal rights of citizens (Article 161), violation of the secrecy of correspondence (Article 163), extortion (Article 189), causing property damage by deception (Article 192), terrorist activities (articles 258-2, 258-4), encroachment on state symbols

[1] Council of Europe Convention on Cybercrime. (2001, November). Retrieved from https://surl.lt/lzzdfv.
[2] Directive of the European Parliament and of the Council No. 2022/2555 "On Measures for a High Common Level of Cybersecurity Across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)". (2022, December). Retrieved from https://www.nis2-info.eu/full-text.
[3] Directive of the European Parliament and of the Council No. 2022/2557 "On the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC". (2022, December). Retrieved from http://data.europa.eu/eli/dir/2022/2557/oj
[4] Law of Ukraine No. 2163-VIII "On the Main Principles of Ensuring Ukraine's Cybersecurity". (2017, May). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text.
[5] Criminal Code of Ukraine. (2001, April). Retrieved from https://kku.com.ua/chastyna-2/rozdil-16/.

(Article 338), and threats or violence against journalists and officials (Article 345-1, Article 350).

Military realities have led to amendments to the current legislation in the field of digital technology protection, in particular, the adoption of laws No. 2137-IX[1] and No. 2149-IX[2], which, on the one hand, simplified the order the collection and verification of evidence, including in proceedings related to countering cybercrime, and on the other hand, determine a number of issues regarding the proportionality of interventions to restrict human rights (most of the changes made contain general, not special (under martial law) norms). Article 361 of the Criminal Code of Ukraine,[3] "Unauthorised interference in the operation of information (automated), electronic communication, information and communication systems, electronic communication networks", which updates the terminology and classification of crimes provided for in Article 361 (replacing the outdated "electronic computing machines (computers)" with "information (automated) systems". There were also changes in terminology, which are reflected in the Law of Ukraine "On electronic communications"[4], provides for the use of the terms "information, automated systems, electronic communications and communication systems" instead of "computers, automated systems, computer networks and telecommunications networks". This is done in accordance with other laws of Ukraine related to cybersecurity.

According to the cybersecurity strategy of Ukraine[5], key challenges and cyber threats include: the active use of cyber tools in international competition, which increases the risk of cyber-attacks on state and critical infrastructure; the rapid development of information and communication technologies, in particular, cloud and quantum computing, 5G networks, Big Data, the Internet of Things, artificial intelligence, etc., which creates a competitive nature of the development of cybersecurity tools and complicates the adaptation of defence mechanisms; the militarisation of cyberspace and the development of cyber weapons, which makes it possible to secretly conduct cyber-attacks to support combat operations, intelligence and subversion and influence on strategic objects unsystematic introduction of new technologies, digital services, and mechanisms of electronic interaction of citizens with the state, which is carried out without proper assessment of cyber risks and security measures, which increases the vulnerability of state systems.

Therefore, under Ukrainian law, information crimes can take various forms and be committed in various ways. In addition, the actions of cybercriminals are often complex and combine several interrelated offences (Dumchykov, 2022). In the security sector of Ukraine, there is a full range of major "classic" cybercrimes, and their number is growing almost 2.5 times every year. Ukraine is a participant in the world's first cyber war, which poses one of the greatest threats to its and global cybersecurity, using a combination of actions in cyberspace and psychological information operations as part of a hybrid war. There is no single point of view on the term "cyber war" among researchers, and it has not received a single definition in Ukrainian legislation. It is mainly defined as the latent influence of information on individual, group, and mass consciousness through propaganda methods, disinformation, and manipulation to form new views on the socio-political organisation of society (Dmytruk *et al.*, 2022), through convergent threats (threats that combine financial, political and propaganda motives) to create a real danger of cyberterrorist attacks and sabotage on national information systems (Chaplyk, 2020; Antoshchuk & Luchyk, 2025). There are different types of cyber-attacks, including massive and targeted ones. All of them are aimed at state resources and critical facilities. Russian cyber-attacks ignore any rules, affecting infrastructure, humanitarian organisations, private and state-owned enterprises. Russian hackers do not recognise borders and restrictions, attacking various states if they help Ukraine.

Of particular danger is the activities of organised cybercrime groups that carry out targeted attacks on critical infrastructure, financial institutions, and government systems. Both transnational criminal networks and state structures of authoritarian regimes are actively involved in this process, using cyberspace for espionage, data theft, and destabilisation of political processes. The most common types of attacks remain ransomware (ransomware by encrypting data), phishing, and malware, which are constantly being improved, significantly complicating

[1] Law of Ukraine No. 2137-IX "On Amendments to the Criminal Procedure Code of Ukraine and the Law of Ukraine 'On Electronic Communications' to Enhance the Efficiency of Pre-Trial Investigations "Hot on the Trail" and Counter Cyberattacks". (2022, March). Retrieved from https://zakon.rada.gov.ua/laws/show/2137-20#Text.

[2] Law of Ukraine No. 2149-IX "On Amendments to the Criminal Code of Ukraine to Improve the Effectiveness of Combating Cybercrime under Martial Law". (2022, May). Retrieved from https://zakon.rada.gov.ua/laws/show/2149-20#Text.

[3] Criminal Code of Ukraine. (2001, April). Retrieved from https://kku.com.ua/chastyna-2/rozdil-16/.

[4] Law of Ukraine No. 1089-IX "On Electronic Communications". (2020, December). Retrieved from https://zakon.rada.gov.ua/laws/show/1089-20#Text.

[5] Decree of the President of Ukraine No. 447/2021 "On the Decision of the National Security and Defense Council of Ukraine of 14 May 2021 "On the Cybersecurity Strategy of Ukraine". (2021, August). Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#Text.

their detection and neutralisation even for highly qualified specialists.

Along the way, it should be noted that during the war, Ukrainians have become more emotionally vulnerable, and scammers use this to adjust their schemes to current problems (Chekmaryova, 2024). For online fraud, they use computers, phones, and other devices to collect and view data (Chaplyk, 2020). Despite the technological complexity of advanced threats, up to 60% of incidents are caused by the human factor and begin with the opening or downloading of malicious content. In 2025, with the extreme intensification of the introduction of AI in criminal activities and the availability of Ransomware-as-a-Service (RaaS), Phishing-as-a-service (PhaaS), AI-aided attack suites, this trend only increased – there was a "psychologically accurate" phishing with the personalisation of the target in each letter or message.

The Russian Federation is constantly increasing its offensive cyber arsenal, which can cause serious and irreversible destruction, first of all, of the information systems of state bodies of Ukraine and critical information infrastructure facilities, in order to disable them, gain hidden control, and conduct intelligence operations. In addition, they are used for information influence on the population, interference in elections, etc. Its integral part is the so-called "black" hackers. The significance of the "hacking" depends on the context and motivation of its use. Hackers are motivated by various factors, such as social justice, lucrative hacking, or political beliefs. This motivation affects their future goals and actions. Negative hacking can lead to cybercrime, such as identity theft, fraud, cyber-attacks, etc. Some hackers can break into users' personal information space and privacy. Most hacking activities are illegal and can have serious legal consequences (Datsenko & Yavorska, 2023). In particular, within hacker communities, this type of cybercriminal can be distinguished as political cybercriminals. An example is the hacking activity of Russian cybercriminals since 2014, which has become especially active with the beginning of a full-scale invasion. However, during the war years, its goals underwent certain transformations. Thus, for example, if at the beginning of a full-scale invasion, Russian cyber-attacks were aimed at the Ukrainian military and the authorities, then later the focus shifted to causing as much harm as possible to the civilian population.

The aggravation of cyber threats is increasingly manifested in the field of disinformation campaigns and cyber espionage, which poses a serious challenge to national security and socio-political stability of the state. The ENISA Threat Landscape (2025) report contains information on almost 5 thousand confirmed cases of cyber violations in EU member states, which indicates their consistency. For this purpose, a network environment is created in which the interests of states and criminal structures intersect. There is a gradual transition from single attacks to "strategic influence operations", which acquire a complex character, combining elements of information manipulation, espionage, destabilisation, etc.

In response to these challenges, the government of Ukraine is taking active measures to strengthen cyber defence. Thus, the State Special Communications Service has introduced new legislative initiatives. By Order No. 54[1] of 30 January 2025, it approved the Basic Cybersecurity Measures and Methodological Recommendations for Implementing Basic Cybersecurity Measures, which introduced the updated Cybersecurity Framework (CSF) 2.0 of the US National Institute of Standards and Technology (NIST). In this regard, M.M. Chaplyk (2020) highlighted the cyberfront in hybrid wars, which are attributed to a new type of war, where economic motives often fade into the background. The concept of cyber front encompasses large-scale attacks on government agencies, information systems, law enforcement agencies, enterprises and critical infrastructure, including cyber espionage and disinformation dissemination, including deepfakes created by AI for mass manipulation of consciousness.

Furthermore, the current Criminal Procedure Code of Ukraine[2] does not contain the concept of "electronic evidence", unlike, for example, the Civil Procedure Code of Ukraine[3] (Article 100). But the legislator suggests considering computer data as a document (paragraph 2 of Article 99 of the Criminal Procedure Code[4]). However, a document is a permanent, fixed material object, while computer data can be quickly changed or deleted, including remotely. In addition, the way electronic information is displayed largely depends on the software and hardware with which it is viewed. In practice, among researchers (Hutsaliuk, 2025), there is some confusion between the concepts of "electronic evidence" and "electronic document", defined in the Law of Ukraine "On

[1] Order of the State Special Communication Service of Ukraine No. 54 "Basic Cybersecurity Measures and Methodological Recommendations for Implementing Basic Cybersecurity Measures, which Introduce the Updated Cybersecurity Framework (CSF) 2.0 of the National Institute of Standards and Technology (NIST) of the USA". (2025, January).Error! Hyperlink reference not valid. Retrieved from https://ips.ligazakon.net/document/FN086217.

[2] Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/4651-17#Text.

[3] Civil Procedure Code of Ukraine. (2004, March). Retrieved from https://zakon.rada.gov.ua/laws/show/1618-15#Text.

[4] Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/4651-17#Text.

Electronic Documents and Electronic Document Management"[1]. Contemporary international legal instruments in the field of combating cybercrime emphasise the key role of international cooperation and information exchange, in particular, with regard to data stored in electronic form. In addition, the investigation of both traditional and war crimes committed during the aggression of the Russian Federation, in the vast majority of cases, requires the receipt, analysis, and proper storage of electronic evidence, which is critical for establishing the truth and ensuring justice.

Thus, there are the following main threats in the field of cybersecurity in Ukraine:

- hybrid aggression of the Russian Federation in cyberspace;
- active build-up of the aggressor state's arsenal of offensive cyber weapons, the use of which can lead to irreparable and irreversible destructive consequences;
- the focus of Russian cyber-attacks is mainly on information and communication systems of state bodies and objects of critical information infrastructure in Ukraine;
- the use of cyber-attacks as an element of special information operations, which makes it possible to manipulate public opinion, interfere in electoral processes, and discredit Ukrainian statehood;
- damage to information resources, public processes and citizens, undermining confidence in information technologies and significant material losses;
- use of cyberspace to commit crimes against the foundations of national security of Ukraine, including criminal offences related to the legalisation of proceeds from crime, human trafficking, illegal trafficking in weapons, military supplies, explosives, and narcotic drugs;
- organised and government-sponsored cyberattacks of other states, the purpose of which is to steal sensitive information for political, economic or military purposes (cyber espionage);
- intelligence and subversive activities aimed at destabilising state and economic systems.

All these cyber threats are extremely difficult to counter and require continuous improvement of both technological solutions and strategies aimed at protecting information systems and data. Nowadays, it is advisable to build a system of response and protection based on an integrated approach to risk assessment, which provides for the introduction of comprehensive methods for analysing cyber threats in the technological, economic, political, legal, and environmental spheres, in particular through institutional integration with the ENISA-CERT system to expand the exchange of intelligence data on threats, which would allow for a more detailed assessment of hazards and timely application of effective counteraction measures. Simultaneously, current challenges in the field of cybersecurity make it necessary to develop theoretical foundations, which involves the development of new approaches to understanding and assessing risks, studying current trends, analysing the characteristics of threats and possible consequences, and developing methodological foundations for managing cyber risks. The growing number of cyber incidents actualises the creation of new cyber defence concepts focused on updating security strategies and approaches, developing innovative technologies, implementing modern standards, improving professional training of specialists, and expanding partnerships between government agencies and the private sector, improving the level of protection of critical infrastructure in accordance with the requirements of NIS2. Cyber defence should be based on a comprehensive combination of technological, organisational, and legal measures, including the introduction of advanced security systems, improvement of security management mechanisms, compliance with legal requirements, and the development of a security culture both in organisations and in society as a whole (Haiduk & Zverev, 2024), in connection with which the development of scientific and educational initiatives in the field of cyber defence is of particular importance.

All of the above measures constitute a cybersecurity strategy. Cybersecurity as a counteraction to cybercrime is a state of protection of key interests of the individual, society, and the state during the use of computer systems and networks, which minimises damage from incomplete or unreliable information, negative information impact, adverse consequences of it, and unauthorised access or violation of the integrity, confidentiality, and availability of data.

In the global dimension, cybersecurity consists of implementing a set of measures aimed at protecting networks, software, and information systems from digital attacks. Such protection covers preventive actions, including regular software updates, the use of complex passwords and multi-factor authentication, and training citizens in basic cybersecurity rules. An important role is played by regulatory measures that provide for the development and continuous improvement of legislation in the field of countering cybercrime. An integral element is international cooperation, which consists in the exchange of information about cyber threats, joint identification and suppression of cybercriminals, and the creation of specialised law enforcement units to investigate

[1] Law of Ukraine No. 851-IV "On Electronic Documents and Electronic Document Management". (2003, May). Retrieved from https://zakon.rada.gov.ua/laws/show/851-15/ed20030522#Text.

cybercrime. However, the development of new security technologies, in particular encryption, incident mining, and other innovative solutions, and ensuring the ethical use of information technologies by adhering to appropriate standards and preventing their criminal use, is of great importance.

According to Ukrainian legislation, cybersecurity is the protection of vital interests of a person and citizen, society, and the state in the process of using cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention, and neutralisation of real and potential threats to the national security of Ukraine in cyberspace (paragraph 5, part 1, Article 1 of the Law of Ukraine "On the Main Principles of Ensuring Ukraine's Cybersecurity"[1]).

Information security in Ukraine is becoming of key importance as an integral component of the national security of the state. This, in turn, involves the adoption of special laws that regulate access to information, personal data protection, countering cybercrime, and control over media and social networks. Martial law requires the introduction of additional measures aimed at restricting access to certain types of information, controlling media and Internet platforms, and protecting critical information infrastructures from risks (Sashchenko, 2022). The legislation should also provide for the development and application of the latest technologies, in particular, AI for preventing cyber-attacks, and other innovative methods of protecting information resources.

The development and implementation of state policy in the field of preventing and countering cybercrime are processes carried out within the national cybersecurity system and can be considered from the standpoint of organisational legal, organisational technical, and law enforcement aspects. There is a growing need for state interaction with society and the international community in order to overcome this negative phenomenon (Kravtsova, 2018), in particular, the implementation of national legislation in the international creation of a common cybersecurity platform for rapid information exchange since cybercrime daily threatens global peace, security, and stable development of international relations (Karvatska *et al.*, 2025).

Cyber-attacks often cover several countries, which makes them difficult to investigate and prevent. A centralised system for sharing data on cyber-attacks, new criminal methods, and vulnerabilities will allow states to jointly respond quickly to threats. Such a platform can provide analytical reports, warnings about new attacks, and recommendations for government and business. International cooperation in the field of countering cybercrime is complicated due to the different vision of this problem by the states of the world, which is conditioned by different approaches to defining key concepts, blurred differentiation of various phenomena that require verified cooperation mechanisms, differences in approaches to ensuring the security of personal data, and a high level of mutual distrust that hinders cross-border partnership.

Conclusions

The subject of research was the investigation of the phenomenon of cybercrime in the current state in the context of the risks that this phenomenon poses for global security and security of Ukraine during the Russian-Ukrainian war, its features, main areas of counteraction against the background of modern realities were highlighted, an analysis of Ukrainian and international legislation in this area, etc., was carried out, as a result of which a number of conclusions were drawn.

Having considered the technical and socio-legal aspects of the phenomenon of cybercrime, it can be argued that at the moment it is impossible to completely eliminate cyber threats due to their intensive and continuous technological development, but it is necessary to develop an adaptive mechanism that will include raising security standards through a multi-level system of redundancy and segmentation of networks, threat intelligence sharing, creating a global secure cyberspace, applying special educational programmes, etc.

The analysis of international legislation showed that the international legal framework in the field of cybersecurity with the development of information technologies requires constant updating (for example, it is necessary to regulate the use of artificial intelligence at the legislative level); inconsistency of regulation and approaches to cyber defence in different countries of the world significantly complicate the consolidation of efforts in the fight against cybercrime, countering cyber threats and cyber-attacks, which have become an integral part of hybrid wars. It is also important to unify the conceptual framework for adapting international legislation to new challenges in the field of cybersecurity.

Ukrainian lawmakers of the Criminal and Criminal Procedure Codes of Ukraine have made the necessary changes to the legislation, supplementing laws and regulations with articles that, among other things, specify the liability for certain types of cybercrimes, which makes it possible to avoid legal conflicts in the classification of crimes and comply with certain rules of procedural law, in particular, with

[1] Law of Ukraine No. 2163-VIII "On the Main Principles of Ensuring Ukraine's Cybersecurity". (2017, May). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text.

regard to covert investigative (search) activities in the digital environment. It was concluded that these changes are appropriate and timely, with the caveat that the introduction of full, total censorship even in wartime does not seem acceptable. In a democratic state, the authorities must guarantee the observance of democratic rights and freedoms even in wartime. Therefore, it is necessary to create an effective mechanism that would ensure state information security and respect for human rights, while simultaneously allowing people not to feel the effect of encroachments on freedoms and democracy.

In the course of the study, it was found that cybersecurity should be deeply integrated into the global security system, since, as already noted, cybercrime is transnational in nature and can have a destructive impact on the political, economic, and social stability of states. Moreover, Ukraine currently has a number of systemic problems, such as fragmented cyber defence policies, uncoordinated actions with partner states (NATO, the European Union, the United States, Great Britain, and Canada), and inefficient use of international technical assistance received from them aimed at strengthening cyber resilience, in particular, irrational use of cyber defence software and hardware received within the framework of international technical assistance. Thus, the issue of developing a national model for ensuring cybersecurity of enterprises, institutions and organisations, including non-governmental ones, coordination of efforts and interaction of law enforcement agencies, special services, the judicial system, and their proper personnel and material and technical support, exchange of information on preventing and combating cybercrime, in particular, the development of conceptual approaches to the implementation of state policy in the field of ensuring the rights of citizens in cyberspace (especially the most vulnerable groups of the population, especially children), the development of a culture of cyber hygiene, etc., becomes relevant.

The problem of cybercrime requires constant attention of scientists, in particular, research should be carried out in the areas of countering cyber violations and cybercrime, network wars, creating a secure cyberspace that includes the protection of information systems, networks and technologies, improving legal regulation, both at the international level and at the level of individual states, developing new concepts of comprehensive cybersecurity, etc.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Antoshchuk, S.A., & Luchyk, V.E. (2024). Cyberfraud in Ukraine in the conditions of war. In *Information and analytical support for the activities of the security and defense sector of Ukraine*: *Materials of the scientific and practical conference* (pp. 4-6). Lviv: Lviv State University of Internal Affairs.

[2] Chaplyk, M.M. (2020). Ukrainian dimension of cybercrime through the prism of certain types of cybercriminals. *Habituss*, 11, 83-87. doi: 10.32843/2663-5208.2020.11.14.

[3] Chekmaryova, I.M. (2024). Internet fraud as one of the types of fraud. *Analytical and Comparative Jurisprudence*, 2, 639-643. doi: 10.24144/2788-6018.2024.02.106.

[4] Datsenko, A.V., & Yavorska, T.M. (2023). Hacking as a phenomenon of the information society. *Bulletin of the Student Scientific Society*, 15(2), 184-187.

[5] DeMillo, A., & Spafford, E.H. (2025). Grand challenges in trustworthy computing at 20: A retrospective look at the second CRA grand challenges conference. *Communications of the ACM*, 68(9), 54-61. doi: 10.1145/3720534.

[6] Dioriditsa, I. (2017). Classification of cyber threats and their legitimisation in the normative legal acts of Ukraine. *Entrepreneurship, Economics, Law*. *Criminal Law*, 10, 206-211.

[7] Dmytruk, Y.V., Hryshanovych, T.O., Hlynchuk, L.Y., & Zhyharevych, O.K. (2022). Cyberwar as a variety of information wars. *Cybersecurity: Education, Science, Technique*, 4(16), 28-36. doi: 10.28925/2663-4023.2022.16.2836.

[8] Dolia, E. (2024). Analysis of contemporary scientific thought on the study of the development and counteraction of cybercrime. *International Science Journal of Engineering & Agriculture*, 5, 93-102. doi: 10.46299/j.isjea.20240305.09.

[9] Dolzhenko, L.Yu. (2020). Cybercrime: Forensic characteristics and features of investigation. *Young Scientist*, 5(81), 219-223. doi: 10.32839/2304-5809/2020-5-81-45.

[10] Dovzhenko, O.Yu. (2019). Classification of cybercrimes in forensic science. *Southern Ukrainian Legal Journal*, 1, 19-23. doi: 10.32850/sulj.2019.1-5.

[11] Dulepa, V.P. (2021). Criminological characteristics of cybercrime. *Legal Scientific Electronic Journal*, 11, 592-595. doi: 10.32782/2524-0374/2021-11/147.

[12] Dumchykov, M.O. (2022). Criminal-legal characteristics of the concept and types of cybercrime. *Scientific Bulletin of the International Humanitarian University*, 55, 65-68. doi: 10.32841/2307-1745.2022.55.14
[13] Dykyi, A., Savitsky, V., Savchuk, S., & Sokha, A. (2025). Global trends in cybercrime and threats to national information security. *Society and Security*, 1(7), 63-74. doi: 10.26642/sas-2025-1(7)-63-74.
[14] ENISA Threat Landscape 2025. (2025). Retrieved from ttps://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.
[15] Fedorenko, T.V., & Fedorenko, V.V. (2023). Main provisions of cyberspace: Concept and essence. *Modern Scientific Journal*, 2(2), 68-71. doi: 10.36994/2786-9008-2023-2-9.
[16] Haiduk, O.V., & Zverev, V.P. (2024). Analysis of cyber threats in the context of rapid development of information technology. *Cybersecurity. Education, Science, Technique*, 3(23), 225-234. doi: 10.28925/2663-4023.2024.23.225236.
[17] Hutsaliuk, M.V. (2025). Cyber threats during hybrid warfare and counteraction to organized cybercrime. *Information and Law*, 1(52), 123-131. doi: 10.37750/2616-6798.2025.1(52).324708.
[18] Karvatska, S.B., Manyk, A.Z., & Stroich, M.I. (2025). Cybersecurity: Modern challenges and international legal frameworks for data protection. *Scientific Bulletin of Uzhhorod National University*, 87(4), 251-256. doi: 10.24144/2307-3322.2025.87.4.39.
[19] Krasko, M.I., & Tsevukh, A.I. (2025) Evolution of cybercrime: How criminal law adapting to the digital era. *Analytical and Comparative Jurisprudence*, 3(2), 387-393. doi: 10.24144/2788-6018.2025.03.2.63
[20] Kravtsova, M.O. (2018). The current state and directions of countering cybercrime in Ukraine. *Bulletin of the Criminal Law Association of Ukraine*, 2(19), 155-166.
[21] Nedilko, Y.V. (2018). The concept of cybercrimes and their types. *Scientific Journal of the National Academy of Prosecution of Ukraine*, 4, 49-60.
[22] Sashchenko, M.I. (2022). Problematic aspects of preventing cybercrime in Ukraine. *Young Scientist*, 1(101), 17-20. doi: 10.32839/2304-5809/2022-1-101-4.
[23] Shak, R. (2024). The concept and types of cyber offenses in criminal law. *Bulletin of the National University "Lviv Polytechnic"*, 4(44), 325-335. doi: 10.23939/law2024.44.325.
[24] Spafford, E.H., Metcalf, L., & Dykstra, J. (2023). *Cybersecurity myths and misconceptions: Avoiding the hazards and pitfalls that derail us*. Boston: Addison Wesley Professional.

Кіберзлочини: аналіз нових викликів і правових механізмів протидії

Аліна Чукаєва
Доктор філософії в галузі права, доцент
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0001-8251-5187

■ **Анотація.** Ситуація поширення гібридних засобів ведення війни сприяє стрімкому збільшенню кількості інформаційних злочинів, різних за формою та способами вчинення, серед яких і такі, що мають комплексний характер. Метою цього дослідження було ґрунтовне критичне осмислення основних підходів до протидії відповідним видам кіберзлочинів. У дослідженні використано системний, порівняльно-правовий, формально-логічний, функціональний методи. Зазначено, що в національному законодавстві з правового регулювання сфери кібербезпеки є низка прогалин, які ускладнюють співпрацю з іншими державами в протистоянні кіберзлочинності та знижують ефективність заходів безпеки, запропоновано шляхи їх усунення. Акцентовано на необхідності впорядкування понятійного апарату, що обслуговує сферу кібербезпеки (наприклад, надання чіткої дефініції поняття кібервійни), а також гармонізації національних правових норм із відповідним міжнародним законодавством з огляду на доцільність уніфікування правових норм різних держав під час регламентації дій сторін для забезпечення ефективності міжнародного співробітництва в боротьбі з кіберзлочинністю. Зауважено, що подолання глобальних проблем кібербезпеки потребує консолідації зусиль держав світу, удосконалення правових і технічних механізмів, утвердження засад культури безпеки в кіберпросторі. Засвідчено необхідність створення ефективного механізму, який водночас гарантував би інформаційну безпеку держави й захищав демократичні права та свободи. Практичне значення отриманих результатів полягає в можливості їх використання для вдосконалення національного законодавства у сфері кібербезпеки та протидії кіберзлочинності, зокрема під час розроблення і коригування нормативно-правових актів відповідно до вимог міжнародного права та положень Будапештської конвенції

■ **Ключові слова:** кібербезпека; кіберпростір; кібервійна; хакер; інформація; етичні стандарти; міжнародна співпраця