ISSN 2409-6415

Електронне науково-практичне фахове видання



2025 / № 132

Журнал східноєвропейського права

(Протокол № 3 від 08 жовтня 2013 року)
Включено до Переліку наукових фахових видань України
(Наказ Міністерства освіти і науки України від 15.04.2014 № 455)
ISSN 2409-6415
Журнал східноєвропейського права внесений до HeinOnline

Проблематика: висвітлення результатів фундаментальних та прикладних наукових досліджень, дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук з актуальних проблем становлення та прагматичного розвитку східноєвропейського права в умовах глобалізаційних викликів

Галузь науки: юридичні науки

Періодичність: щомісячно

Головний редактор: Мосьондз Сергій Олександрович, доктор юридичних наук, професор, виконуючий обов'язки ректора ПВНЗ «Університет сучасних знань»

Відповідальний секретар: Соколан Тетяна Сергіївна, кандидат юридичних наук

Члени редколегії: **Мельник Роман Сергійович,** доктор юридичних наук, професор, завідувач кафедри адміністративного права, Київський національний університет імені Тараса Шевченка **Янчук Артем Олександрович,** доктор юридичних наук, професор, державний секретар, Міністерство охорони здоров'я, **Кузьменко Оксана Володимирівна,** доктор юридичних наук, професор, професор кафедри теорії та історії права, Державний вищий навчальний заклад «Київський національний економічний університет імені Вадима Гетьмана», **Личенко Ірина Олександрівна**, доктор юридичних наук, професор, завідувач кафедри цивільного права та процесу, Навчально-науковий інститут права, психології та інноваційної освіти Національного університету «Львівська політехніка», **Чорна Вікторія Григорівна,** доктор юридичних наук, доцент, доцент кафедри адміністративного права і процесу, Державний вищий навчальний заклад «Київський національний економічний університет імені Вадима Гетьмана», **Губанова Тамара Олексіївна,** доктор юридичних наук, професор, директор, Приватний вищий навчальний заклад «Фінансово-правовий коледж», **Книш Сергій Володимирович,** кандидат юридичних наук, юрисконсульт, Східноєвропейський національний університет імені Лесі Українки, **доктор Егле Білевічюте,** член Комісії з розгляду адміністративних спорів Литви, професор Університету Миколаса Ромеріса, (Вільнюс, Литва), **доктор Тома Бірмонтієн,** професор Лабораторії правосуддя, Лабораторії прав людини юридичного факультету Інституту публічного права Університету Миколаса Ромеріса, (Вільнюс, Литва), **доктор Агне Тваронавічієн,** Лабораторія соціальних технологій, Лабораторія посередництва та сталого розв'язання конфліктів юридичного факультету Інституту публічного права Університету Миколаса Ромеріса (Вільнюс, Литва)

Адреса редакції: вул. Велика Васильківська, 57/3, м. Київ, Україна, 03150

Тел.: +38 (063) 758 57 24
E-mail: easternlaw.ua@gmail.com
Сайт: http://easternlaw.com.ua

(Order of the Ministry of Education and Science of Ukraine of 15.04.2014 No. 455)
ISSN 2409-6415
The Journal of Eastern European Law is included in HeinOnline

Issue: lighting the results of basic and applied research, dissertations for the degree of doctor and candidate of sciences on current issues of establishment and pragmatic development of Eastern European law within globalization challenges

Branch of science: jurisprudence

Frequency: monthly

Editor in Chief: Mosondz Serhii Oleksandrovych, doctor of juridical sciences, professor, acting rector of the Private Higher Educational Establishment "The University of Modern Knowledge"

Secretary in Charge: Sokolan Tetiana Serhiivna, candidate of juridical sciences

Members of the editorial board: **Melnyk Roman Serhiiovych,** doctor of juridical sciences, professor, head of the Department of Administrative Law of Taras Shevchenko National University of Kyiv, **Yanchuk Artem Oleksandrovych,** doctor of juridical sciences, professor, state secretary, the Ministry of Health, **Kuzmenko Oksana Volodymyrivna,** doctor of juridical sciences, professor, professor of the Department of theory and history of law at the State Higher Educational Establishment "Kyiv National Economic University named after Vadym Hetman", **Lychenko Iryna Oleksandrivna,** doctor of juridical sciences, head of the Department of Civil Law and Procedure at the Training and Scientific Institute of Jurisprudence, Psychology and Innovative Education of Lviv Polytechnic National University, **Chorna Viktoriia Hryhorivna,** doctor of juridical sciences, associate professor, associate professor of the Department of Administrative Law and Proceeding at the State Higher Educational Establishment "Kyiv National Economic University named after Vadym Hetman", **Hubanova Tamara Oleksiivna,** doctor of juridical sciences, professor, director at the Private Higher Educational Establishment "Financial and Law College", **Knysh Serhii Volodymyrovych,** candidate of juridical sciences, legal counsel, Lesya Ukrainka Eastern European National University, **Dr. Eglė Bilevičiute,** member at Lithuania Administrative Disputes Commission, professor at the Mykolas Romeris University (Vilnius, Lithuania), **Dr. Toma Birmontien,** professor at Justice Laboratory, Human Rights Laboratory of Faculty of Law of Institute of Public Law, Mykolas Romeris University (Vilnius, Lithuania), **Dr. Agne Tvaronaviciene,** Social Technologies Laboratory, Mediation and Sustainable Conflict Resolution Laboratory of Faculty of Law, Institute of Public Law of Mykolas Romeris University (Vilnius, Lithuania).

Address of the editorial office: 57/3 Velyka Vasylkivska Street, Kyiv, 03150, Ukraine

Tel.: +38 (063) 758 57 24
E-mail: easternlaw.ua@gmail.com
Website: http://easternlaw.com.ua

ЗМІСТ

Мосьондз С.О., Чудненко В.О. Правова природа охорони навколишнього природного середовища……...9

Верхогляд О.В., Стрельченко О.Г. Проблемні питання застосування адміністративної відповідальності у період війни……15

Грібов М.Л. Оперативно-розшукова таємниця як елемент забезпечення інформаційної безпеки……21

Гринько С.Д. Особливості цивільно-правової відповідальності за шкоду, завдану споживачам внаслідок недоліків товарів, робіт (послуг) в умовах гібридної війни в Україні……29

Дідківська Г.В. Проблеми кримінальної відповідальності за кримінальні правопорушення проти довкілля: міжнародний досвід……39

Дорошенко Л.М. Судовий активізм: бути чи не бути… ……46

Кириленко Л.О., Стрельченко О.Г. Адміністративне судочинство: спосіб захисту порушених прав та інтересів чи втручання у повноваження суб'єкта владних повноважень……..61

Кириченко О.А. Конституційні основи докорінного реформування президентатури, прокуратури, публічнотури і всієї іншої системи антиделіктних органів в контексті розбудови правової держави гуманізму будь-якої держави світу……69

Проневич О.С., Коляда Т.А. Органи виконавчої влади як суб'єкти нормотворчої діяльності у сфері обігу медичного канабісу……85

Теремецький В.І., Риженко О.С. Адміністративна відповідальність медичних працівників за правопорушення, вчинені під час виконання професійних обов'язків……98

Щербакова Н.В. Питання визначення моменту виникнення реорганізаційних правовідносин між юридичними особами корпоративного типу……..108

Андрусишин Р.М. Поняття, зміст та функції правового виховання працівників Національної поліції в Україні……...123

Бойко І. Зміст, передумови виникнення та структурні елементи митних деліктів: теоретико-правовий аналіз……136

Бухтіярова І.Г., Оземха І.В. Використання штучного інтелекту у державному управлінні: адміністративно-правові аспекти……...143

Глух М.В., Єфіменко О.А. Теоретико-правові засади фінансового контролю за місцевими фінансами……151

Гулкевич З.Т. Розвиток інноваційного розуміння сутності, базисних ознак, видового поділу та іншої класифікації механічної зброї та/чи боєприпасів та слідів протиправного поводження з ними.....159

Кобець О.А., Сошников А.О. Некомерційне господарювання vs соціальне підприємництво: сучасні реалії та підходи……..173

Лаговська Н.В., Фірскіна К.М. Проблеми та перспективи розвитку інституту опіки та піклування в Україні під час воєнних дій……...184

Ланцедова Ю.О. Інноваційне розуміння міждисциплінарної сутності, послідовності та інших закономірностей роботи із суб'єктивними, об'єктивними та змішаними джерелами антиделіктних відомостей в контексті забезпечення верховенства права……..191

Лапка О.Я., Славна О.В. Мирні способи врегулювання міжнародних конфліктів у контексті війни України та РФ…….204

N.A. Luhina, O.M. Paliukh Legal Challenges of International Cooperation in Combating Cybercrime: Prospects for Improving the Regulatory Framework…….214

Лях Н.В. Захист прав дітей в умовах війни – міжнародний досвід ……...219

Рощина І.О., Кришевич О.В. Кримінальна відповідальність як гарантія захисту незалежності судової влади в Україні……232

Сукмановська Л.М., Репан М.І. Дослідження особливостей роботи підрозділів Національної поліції із дітьми, що постраждали від домашнього насильства……...238

Тунтула О.С. Розвиток інноваційного розуміння сутнісного видового поділу об'єктивних, суб'єктивних та змішаних джерел відомостей в антикримінальному та іншому антиделіктному судочинстві……...245

Барбара О.С. Міжнародний досвід державного регулювання зовнішньоекономічної діяльності в умовах воєнного стану: досвід для України……..261

Дехтяр Б.С. Застосування заходів забезпечення кримінального провадження за рішенням слідчого судді……...269

Клименко І.Ю. Досвід зарубіжних країн у запобіганні організованої злочинності неповнолітніх……...275

Петер Г.Г. Характеристика кримінологічного забезпечення міжнародної космічної діяльності у сфері протидії космічним небезпекам в умовах міжнародних розбіжностей та військових конфліктів……281

Челомбітко С.М. Інноваційне розуміння хронології розвитку, напрямків, поняття, системи і дисциплінарного статусу одорології як базисного часткового вчення криміналістики та ордистики (присвячується пам'яті В.Д. Басая)……..292

Шаповалова К.І. Роль Національної поліції України у створенні безпечного освітнього середовища……...308

Яцюк С.О. Застосування запобіжних заходів в умовах воєнного стану ……...323

TABLE OF CONTENTS

S.O. Mosondz, V.O. Chudnenko Legal Nature of Environmental Protection ……...9

O.V. Verkhohliad, O.H. Strelchenko Problem Issues of the Application of Administrative Liability in War Times……15

M.L. Hribov Operational-Search Secrecy as an Element of Information Security Ensurement……..21

S.D. Hrynko Features of Civil Liability for Damage Caused to Consumers as a Result of Deficiencies in Goods, Works (Services) in the Context of Hybrid War in Ukraine……29

H.V. Didkivska Problems of Criminal Liability for Criminal Offenses against the Environment: International Experience……..39

L.M. Doroshenko Judicial Activism: to Be or Not to Be… ……46

L.O. Kyrylenko, O.H. Strelchenko Administrative Judicial Proceedings: a Method of Protecting Violated Rights and Interests or Interference with the Powers of an Authority……..61

O.A. Kirichenko Constitutional Foundations for the Radical Reform of the Presidencytura, Prosecutura, Publictura and the Entire other System of Antidelictal Authorities in the Context of Building a Legal State of Humanism in Any State in the World……...69

O.S. Pronevych, **T.A. Koliada** Executive Authorities as Subjects of Regulatory Activity in the Sphere of Medical Cannabis Circulation……85

V.I. Teremetskyi, O.S. Ryzhenko Administrative Liability of Medical Workers for Offenses Committed During the Performance of their Professional Duties……98

N.V. Shcherbakova Issues of Determining the Moment of Emergence of Reorganization Legal Relations between Corporate-Type Legal Entities……108

R.M. Andrusyshyn Concept, Content and Functions of Legal Education of National Police Officers in Ukraine……...123

I. Boiko Content, Prerequisites for Emergence, and Structural Elements of Customs Offenses: a Theoretical and Legal Analysis……..136

I.H. Bukhtiiarova, I.V. Ozemkha The Use of Artificial Intelligence in Public Administration: Administrative and Legal Aspects……..143

M.V. Glukh, O.A. Yefimenko Theoretical and Legal Basis of Financial Control over Local Finances……151

Z.T. Gulkevich Development of Innovative Understanding of the Essence, Basic Characteristics, Species Division and Other Classification of Mechanical Weapons and/or Armaments and Trails of Illegal Handling of Them.....159

O.A. Kobets, A.O. Soshnykov Non-Commercial Economic Activity vs. Social Entrepreneurship: Modern Realities and Approaches……173

N.V. Lagovska, K.M. Firskina Problems and Prospects of Development of the Institute of Care and Guardianship in Ukraine during the War……184

Yu.A. Lantsedova An Innovative Understanding of the Interdisciplinary Nature, Sequence, and Other Patterns of Working with Subjective, Objective and Mixed Sources of Antidelictal Information in the Context of Ensuring the Rule of Law……191

O.Ya. Lapka, O.V. Slavna Peaceful Ways of Resolving International Conflicts in the Context of the War between Ukraine and the Russian Federation……204

N.A. Luhina, O.M. Paliukh Legal Challenges of International Cooperation in Combating Cybercrime: Prospects for Improving the Regulatory Framework……214

N.V. Liakh Protection of Children's Rights in Wartime – International Experience ……...219

I.O. Roshchina, O.V. Kryshevych Criminal Liability as a Guarantee of Protection of the Independence of the Judiciary in Ukraine……...232

L.M. Sukmanovska, M.I. Repan Study of the Features of the Work of the National Police Units with Children who Have Suffered from Domestic Violence……..238

O.S. Tuntula Development of an Innovative Understanding of the Essential Species Division of Objective, Subjective and Mixed Sources of Information in Anticriminal and Other Antidelictal Proceedings……245

O.S. Barbara International Experience of State Regulation of Foreign Economic Activity under Martial Law: Experience for Ukraine……261

B.S. Dekhtyar Application of Measures to Secure Criminal Proceedings by Decision of the Investigating Judge……269

I.Yu. Klymenko Experience of Foreign Countries in Preventing Organized Juvenile Crime…….275

H.H. Peter Characteristics of Criminological Safeguards in International Space Activities for Countering Space Threats in the Context of International Disputes and Armed Conflicts…….281

S.M. Chelombitko Innovative Understanding of the Chronology of Development, Directions, Concepts, System and Disciplinary Status of Odorology as a Basic Partial Doctrine of the Criminalistics and of the Ordistics (Dedicated to the Memory of V.D. Basai)……..292

K.I. Shapovalova The Role of the National Police of Ukraine in Creating a Safe Educational Environment……...308

S.O. Yatsiuk Application of Precautionary Measures under Martial Law ……...323

UDC 341.4:343:004.

Nataliia A. Luhina –
Candidate of Juridical Sciences, Associate Professor,
Associate Professor of the Department of Criminal Law and Procedure,
State Tax University
ORCID: https://orcid.org/0000-0001-6005-2943

Oleksandr M. Paliukh –
Candidate of Economic Sciences,
1st Level Bachelor's Degree Seeker,
State Tax University
(31 Universytetska Street, Irpin,08250, Ukraine)
ORCID: https://orcid.org/0000-0002-9459-2187

Legal Challenges of International Cooperation in Combating Cybercrime: Prospects for Improving the Regulatory Framework

У статті розглядаються сучасні правові виклики міжнародного співробітництва у боротьбі з кіберзлочинністю, зокрема в умовах військових конфліктів та гібридних загроз. Досліджено особливості використання кіберзброї як інструмента гібридної війни та її вплив на глобальну безпеку, національні інтереси держав та критичну інфраструктуру. Проведено комплексний аналіз існуючих міжнародних правових інструментів, таких як Будапештська конвенція про кіберзлочинність, їхніх системних обмежень та перспектив модернізації в контексті новітніх кіберзагроз. Особливу увагу приділено проблемам гармонізації національних законодавств, координації оперативних дій між державами та розробці ефективних механізмів правового регулювання кіберпростору. Висвітлено унікальний досвід України як держави, що зазнає масштабних кібератак в рамках військової агресії, її роль у глобальному співробітництві та практичний досвід у протидії кіберзагрозам різного рівня складності. Обґрунтовано необхідність створення універсальних міжнародних стандартів для екстрадиції кіберзлочинців, обміну інформацією між компетентними органами різних держав та вдосконалення механізмів захисту жертв кіберзлочинів. Запропоновано конкретні шляхи вдосконалення міжнародно-правової бази для забезпечення ефективної боротьби з кіберзлочинністю на глобальному рівні з урахуванням сучасних технологічних, політичних та безпекових викликів.

Ключові слова: *кіберзлочинність, міжнародне співробітництво, кібербезпека, Будапештська конвенція, гармонізація законодавства, гібридна війна, кіберзброя, екстрадиція, критична інфраструктура, транскордонні кіберзлочини.*

The article examines contemporary legal challenges of international cooperation in combating cybercrime, particularly under the conditions of armed conflicts and hybrid threats. It investigates the distinctive features of cyberweapons as sophisticated tools of hybrid warfare and analyzes their profound impact on global security, national interests, and critical infrastructure protection. The study provides a comprehensive analysis of existing international legal frameworks, such as the Budapest Convention on Cybercrime, their systemic limitations, and prospects for modernization in the context of emerging cyber threats. Special attention is given to crucial issues of harmonizing national legislation, coordinating operational actions among states, and developing effective mechanisms for legal regulation of cyberspace. The article highlights Ukraine's unique experience as a state facing large-scale cyberattacks as part of military aggression, its evolving role in global cooperation, and practical experience in countering cyber threats of varying complexity. The research substantiates the necessity of establishing universal international standards for the extradition of cybercriminals, information exchange between competent authorities of different states, and improving protection mechanisms for victims of cybercrimes. Furthermore, the article addresses the importance of strengthening international interaction across jurisdictions, ensuring cross-border investigations, and adapting existing norms to the rapidly changing realities of the digital age. The proposed concrete solutions aim to enhance the efficiency of international legal

frameworks in countering cybercrime and ensuring comprehensive global cybersecurity in the context of modern technological, political, and security challenges.

Keywords: *cybercrime, international cooperation, cybersecurity, Budapest Convention, legislative harmonization, hybrid warfare, cyberweapons, extradition, critical infrastructure, cross-border cybercrimes.*

Problem Statement. Modern warfare is characterized by the use of cyber weapons as an integral element of hybrid aggression aimed at destabilizing the critical infrastructure of states, compromising information security, and manipulating public opinion. Cybercrimes, such as unauthorized intrusion into information systems, distribution of malicious software, and cyber espionage, have become instruments of international conflicts. Given the military aggression Ukraine is experiencing, there is an increasing need to improve the legal framework for international cooperation aimed at countering cybercrime and ensuring effective prosecution of offenders. However, the absence of unified mechanisms for legal interaction between states creates significant obstacles in this process.

Analysis of Recent Research and Publications. The topic of international cooperation in combating cybercrime is relevant and actively researched by leading experts in international law, criminal law, and cybersecurity. In their works, authors such as Marushchak A.I. [4], Lysaichuk A.A. [6], and Melnyk M.R. [11] analyze the provisions of the Budapest Convention on Cybercrime, its limitations, and prospects for implementation in Ukraine. An important place in research is occupied by the issue of adapting international agreements to new conditions associated with the use of cyber weapons in wartime.

Reports from international organizations such as the UN [2], Council of Europe [1], and Europol [9] highlight current trends in cybercrime and emphasize the need to strengthen coordination between states. These documents address issues of effective information exchange, improvement of extradition procedures, and combating new forms of cyber attacks that threaten global security. In particular, reports from ENISA [5] and NATO CCDCOE [14] emphasize the growing role of cybercrime as part of hybrid conflicts.

Scientific papers and official documents underscore that effective combating of cybercrime in wartime requires significant changes in the legal and regulatory framework. In particular, attention should be paid to adapting existing international norms to new challenges associated with cyber attacks sponsored by aggressor states.

Unresolved Issues. Despite active research, key problems remain unresolved that hinder effective combating of cybercrime at the global level. Among them are:

1. The absence of a universal international agreement that would regulate mechanisms of state interaction in the field of combating cybercrime [3].
2. Imperfection of extradition procedures for persons suspected of cybercrimes, especially if they are in countries that refuse to cooperate with international organizations [8].
3. Low effectiveness in implementing mechanisms for the exchange of operational information between states [12].
4. The use of cyber attacks as a means of warfare, which requires new approaches to international legal regulation [16].

Purpose of the Article is to comprehensively analyze the legal challenges of international cooperation in combating cybercrime in conditions of military conflicts, to identify the main problems of such interaction, and to develop proposals for improving the regulatory framework for effective counteraction to cyber threats at the international level.

Main Content Presentation. The development of information technology has opened up new horizons for cooperation between states, but at the same time has caused a number of problems related to the spread of cybercrime. This problem is especially acute in times of war, when cybercrime becomes part of hybrid conflicts and is aimed at undermining the functioning of state institutions and critical infrastructure [1, p. 15].

One of the key international documents in the field of combating cybercrime is the Budapest Convention on Cybercrime, which defines legal mechanisms for cooperation between states in the detection, investigation and prosecution of cybercrime. The Convention provides a framework for a joint response to global threats and provides mechanisms for international legal assistance [2]. However, its effectiveness is limited by the fact that a number of states, including key geopolitical players such as China and Russia, are not parties to it [3, p. 45].

The Council of Europe reports state that the Budapest Convention on Cybercrime needs further improvement, in particular in terms of regulating cross-border access to data, as modern cyberattacks are mostly carried out through global networks [1]. In the new conditions of war, the question arises of the need to strengthen the provisions on the responsibility of states for the use of cyber weapons against other countries.

The war in Ukraine has become one of the most striking examples of the use of cybercrime as a means of aggression. Cyberattacks accompanying military operations are aimed not only at destabilizing the internal situation in the country, but also at influencing the international community. For example, in 2022, the Ukrainian energy system suffered large-scale cyberattacks, the consequences of which could have had a catastrophic impact on the population and economy [3].

Such actions require not only a prompt response from the affected country, but also international coordination. In particular, the experience of Ukraine's cooperation with Europol and Interpol in investigating cyberattacks on critical infrastructure confirms the need to expand the legal framework for effective cooperation [9].

One of the biggest obstacles in the fight against cybercrime is the issue of extradition of persons suspected of committing cybercrime. Often, such persons are in states that do not cooperate with international organizations or directly support their activities. For example, the Russian Federation has repeatedly refused to extradite hackers who carried out cyberattacks against the European Union and the United States, making it impossible to bring them to justice [6].

Researchers emphasize that one of the reasons for this situation is the imperfection of international information exchange mechanisms and the lack of unified standards of evidence in cases related to cybercrime. This is especially true for countries with different legal traditions and approaches to evidence collection [4].

Effective counteraction to cybercrime requires harmonization of national legislation with international standards. One example is the European Union's Digital Shield legislative initiative, which envisages the introduction of stricter cybersecurity standards to protect critical infrastructure. Ukraine, as an EU candidate country, is also working to implement these standards in its legislation, which opens up new prospects for cooperation [5].

However, harmonization of legislation does not solve all problems. Effective mechanisms need to be created to ensure prompt access to data on cyberattacks and perpetrators, as well as to ensure rapid interaction between law enforcement agencies of different countries [4].

International organizations play a key role in coordinating efforts to combat cybercrime, especially in the context of military conflicts. For example, Interpol has introduced the Cyber Fusion Center program, which provides for the rapid exchange of information between member countries, the detection of cyber threats, and the coordination of international investigations. This initiative reduces the response time to cyberattacks, which is critical in the current environment [7].

The European Cyber Security Agency (ENISA) develops strategies to protect against cyberattacks, including joint exercises, exchange of experience between EU member states, and the development of standards to protect critical infrastructure. At the same time, ENISA faces difficulties in coordinating with third countries, including Ukraine, due to differences in legal standards and procedural norms [5].

The UN also pays considerable attention to cybersecurity through specialized bodies such as the UN Office on Drugs and Crime (UNODC). The organization promotes the development of unified approaches to investigating cybercrime and providing access to the necessary resources for less developed states [2]. However, the effectiveness of such programs is limited by insufficient funding and political instability in countries in need of assistance.

One of the key aspects of modern cybercrime is the use of cyberweapons by aggressor states as a means of military warfare. Cyberweapons can be conditionally divided into means:

1. Destructive impact on infrastructure (e.g., malware that disrupts power systems).
2. Information theft (cyber espionage).
3. Disinformation (creation and dissemination of fake news to manipulate public opinion) [10, p. 98].

Classical international law does not fully take into account the peculiarities of the use of cyber weapons. For example, the Hague and Geneva Conventions are aimed at regulating armed conflicts,

but do not cover cyberattacks that cause damage without the direct use of physical force. In this context, there is a need to create a special protocol to these conventions or a new international treaty that would regulate the use of cyber weapons in war.

An important factor in combating cybercrime is the financing of relevant measures. The cost of responding to cyberattacks and their consequences can reach hundreds of millions of dollars, as was the case with the NotPetya virus attack that paralyzed businesses in many countries, including Ukraine [11]. International initiatives aimed at reducing economic losses include:

- Creation of funds to support the affected countries;
- introduction of international insurance of risks associated with cyberattacks;
- involvement of the private sector in cooperation through public-private partnerships[12].

However, economic support is not always available to countries at war, which creates additional challenges for their cybersecurity.

Technical and educational support provided by the international community to countries with insufficient training in this area plays a significant role in the fight against cybercrime. Technical assistance programs include training law enforcement agencies in modern methods of investigating cybercrime, as well as providing equipment for monitoring and analyzing data.

Educational initiatives, such as the programs of the European School of Cyber Security, are aimed at forming a new generation of cyber defense specialists. At the same time, UN reports note that the lack of such programs in the face of global demand creates gaps in the protection of many countries [13].

Victims of cybercrime, especially in wartime, are often left without adequate legal protection. For example, the theft of personal data during cyberattacks can lead to financial losses, reputational risks, and even threats to the physical safety of victims. National legislation in most countries does not provide clear mechanisms for compensation for such losses [14].

International practice in this area is limited to isolated initiatives, such as the creation of funds for compensation for losses, but their activities are significantly limited due to insufficient funding and the complexity of legal claims.

Conclusions. Cybercrime, particularly in the context of modern military conflicts, emerges as a global threat that demands an effective legal and organizational response at the international level. The analysis shows that existing legal mechanisms, including international agreements, are not fully capable of responding to new challenges associated with the use of cyber weapons and the complexity of cross-border cybercrimes [15]. The uncertainty of the legal status of such actions, the absence of unified standards in the investigation and punishment of cybercrimes significantly complicate international cooperation.

Special attention must be paid to the harmonization of legislation, as differences in the legal systems of various countries create serious barriers to effective information exchange, evidence sharing, and extradition of suspects. In this context, cooperation between states should be based on clearly regulated mechanisms that ensure operational efficiency and reliability. Military actions in Ukraine have highlighted the critical necessity of strengthening international interaction, particularly in the sphere of information exchange about cyber attacks and identifying the individuals behind these crimes.

Furthermore, technological development requires improving the level of training for specialists in the field of cybersecurity and providing technical support for states that have suffered from cyber attacks. Such initiatives should be accompanied by the development of new international standards aimed at protecting victims of cybercrime, who often remain without proper legal protection. Successful combating of cybercrime is possible only under conditions of a global approach that considers the needs of all states and offers universal solutions for responding to the challenges of the digital age.

References:

1. Budapeshtska konventsiia pro kiberzlochynnist: Konventsiia Rady Yevropy ETS № 185 vid 23 lystopada 2001 roku. URL: https://rm.coe.int/1680081561 (data zvernennia: 20.01.2025).
2. Rezoliutsiia Heneralnoi Asamblei OON “Zabezpechennia bezpeky v kiberprostori” A/RES/73/27 vid 5 hrudnia 2018 roku. URL: https://digitallibrary.un.org (data zvernennia: 20.01.2025).

3. Natsionalna stratehiia kiberbezpeky Ukrainy na 2021–2025 roky: Ukaz Prezydenta Ukrainy № 447/2021 vid 26 serpnia 2021 roku. URL: https://zakon.rada.gov.ua/laws/show/447/2021 (data zvernennia: 20.01.2025).

4. Marushchak A.I. Mizhnarodne spivrobitnytstvo u borotbi z transnatsionalnoiu kiberzlochynnistiu. *Informatsiia i pravo*. 2018. № 3(26). S. 104–110. URL: https://ippi.org.ua/marushchak-ai-mizhnarodne-spivrobitnitstvo-u-borotbi-z-transnatsionalnoyu-kiberzlochinnistyu-st-104 (data zvernennia: 20.01.2025).

5. Cybersecurity Threat Landscape 2023. ENISA Annual Report. URL: https://www.enisa.europa.eu/publications (data zvernennia: 20.01.2025).

6. Lysaichuk A.A. Problemy borotby z kiberzlochynnistiu na mizhnarodnomu rivni. *Visnyk Natsionalnoho universytetu "Ostrozka akademiia". Seriia "Pravo"*. 2015. Vyp. 1(11). S. 1–5. URL: https://evnuir.vnu.edu.ua/bitstream/123456789/11111/1/Lisaychuk%20A.%20A..pdf (data zvernennia: 20.01.2025).

7. Klymenko O.A., Hutsaliuk M.V. Kryminalnyi oportunizm kiberzlochynnosti yak zahroza natsionalnii bezpetsi Ukrainy. *Yurydychnyi visnyk "Povitriane i kosmichne parvo"*. 2020. T. 2. S. 45–50. URL: https://il.ippi.org.ua/article/view/248840 (data zvernennia: 20.01.2025).

8. Yurtaieva K.V. Kryminalna vidpovidalnist za kiberzlochyny, vchyneni pid chas zbroinoho konfliktu: mizhnarodni tendentsii ta ukrainski realii. *Yurydychnyi naukovyi elektronnyi zhurnal*. 2012. № 12. S. 409–414. URL: https://www.lsej.org.ua/12_2012/409.pdf (data zvernennia: 20.01.2025).

9. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2023. URL: https://www.europol.europa.eu (data zvernennia: 20.01.2025).

10. Zhenevski konventsii 1949 roku ta Dodatkovi protokoly do nykh. URL: https://www.icrc.org/uk (data zvernennia: 20.01.2025).

11. Melnyk M.R. Mizhnarodno-pravove spivrobitnytstvo derzhav u borotbi z kiberzlochynnistiu. *Chasopys Kyivskoho universytetu prava*. 2019. № 2. S. 123–128. URL: https://dspace.onua.edu.ua/bitstreams/45584631-74ac-4174-8952-aaa27c92b6e6/download (data zvernennia: 20.01.2025).

12. Feshchukov H.V. Zastosuvannia mizhnarodnoho humanitarnoho prava po vidnoshenniu do kiberoperatsii, shcho provodiatsia pid chas zbroinykh konfliktiv. *Yurydychnyi naukovyi elektronnyi zhurnal*. 2023. № 9. S. 437–439. URL: https://www.lsej.org.ua/9_2023/437.pdf (data zvernennia: 20.01.2025).

13. Yevropeiska konventsiia pro ekstradytsiiu ETS № 24 vid 13 hrudnia 1957 roku. URL: https://rm.coe.int (data zvernennia: 20.01.2025).

14. Kovalenko T.M. Kiberbezpeka v Ukraini: aktualni vyklyky ta mizhnarodnyi dosvid. *Informatsiine pravo*. 2022. № 3. S. 89–102. URL: https://ippi.org.ua (data zvernennia: 20.01.2025).

15. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. NATO CCD COE, 2017. URL: https://ccdcoe.org/tallinn-manual (data zvernennia: 20.01.2025).