

АЛЬМАНАХ МІЖНАРОДНОГО ПРАВА

Випуск 34



Видавничий дім
«Гельветика»
2025

Альманах міжнародного права включено до Переліку наукових фахових видань України (категорія Б) відповідно до Наказу Міністерства освіти і науки України від 24 вересня 2020 р. № 1188 (спеціальності: D8. Право, D9. Міжнародне право)

Засновник видання – Міжнародний гуманітарний університет

Рекомендовано до друку та поширення через мережу Internet Вченою радою Міжнародного гуманітарного університету (протокол № 4 від 03.11.2025 р.)

РЕДАКЦІЙНА КОЛЕГІЯ:

Головний редактор:

Губанова Тамара Олексіївна, доктор юридичних наук, професор, директор, Фінансово-правовий коледж.

Голова редакційної ради:

Громовенко Костянтин Вікторович, доктор юридичних наук, професор, ректор, Міжнародний гуманітарний університет.

Члени редакційної колегії:

Андрейченко Світлана Сергіївна, доктор юридичних наук, доцент, завідувач кафедри міжнародного права та порівняльного правознавства, Міжнародний гуманітарний університет;

Грушко Мальвіна Валеріївна, кандидат юридичних наук, доцент, доцент кафедри міжнародного та європейського права, Національний університет «Одеська юридична академія»;

Діденко Лариса Василівна, доктор юридичних наук, професор, в.о. завідувача кафедри цивільного та господарського права і процесу, Міжнародний гуманітарний університет;

Кізова Олена Сергіївна, доктор юридичних наук, професор, професор кафедри цивільного та господарського права і процесу, Міжнародний гуманітарний університет;

Манько Денис Григорович, доктор юридичних наук, доцент, завідувач кафедри державно-правових дисциплін, Міжнародний гуманітарний університет;

Подобний Олександр Олександрович, доктор юридичних наук, професор, завідувач кафедри кримінального права, процесу та криміналістики, Міжнародний гуманітарний університет;

Тицька Яна Олександрівна, кандидат юридичних наук, доцент, доцент кафедри державно-правових дисциплін, Міжнародний гуманітарний університет;

Цибуленко Євген Миколайович, професор, Таллінська школа права, Естонія.

Партнер журналу

Фінансово-правовий коледж



Реєстрація суб'єкта у сфері друкованих медіа: Рішення Національної ради України з питань телебачення і радіомовлення № 1551 від 09.05.2024 року.

Ідентифікатор медіа: R30-04396

Суб'єкт у сфері друкованих медіа – Міжнародний гуманітарний університет (вул. Фонтанська дорога, м. Одеса, 33, e-mail: priemnayamgu@gmail.com. Тел.: +38 (048) 719-88-38).

Мови розповсюдження: українська, англійська, польська, німецька, французька, іспанська

Періодичність: 2 рази на рік

Статті у виданні перевірені на наявність плагіату за допомогою програмного забезпечення StrikePlagiarism.com від польської компанії Plagiat.pl.

Адреса редакції:

Міжнародний гуманітарний університет
вул. Фонтанська дорога, 33, каб. 402, м. Одеса, 65009, Україна
www.inlawalmanac.mgu.od.ua
Тел. +38 068 938 18 56

МІЖНАРОДНЕ ПРАВО ПРАВ ЛЮДИНИ

УДК 341.3
DOI <https://doi.org/10.32782/ILA.2025.34.01>

КУШНІР В. В.
здобувач вищої освіти
Міжнародного гуманітарного університету
ORCID: 0009-0004-9328-8142

ПРАКТИКА ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ ЯК ФАКТОР ІНФОРМАЦІЙНОЇ ВІЙНИ

Анотація. У статті її автором проведений аналіз особливостей практики Європейського суду з прав людини у вимірі формування європейських правових стандартів поведіння з поширенням інформації як вагомому фактору інформаційної війни, для цього проведено аналіз узагальненої практики Суду стосовно поведінки з інформацією, межі правомірного впливу поширюваної інформації на приватні інтереси людини та правомірну діяльність держави, зокрема у вимірах медіа, зібрань, правоохоронної діяльності та протидії дискримінації.

У статті автором підкреслене, що станом на сьогодні аспекти протидії пропаганді та дезінформації у її різних формах та проявах та форми управлінського й процесуального реагування на такі явища набули для вітчизняної правничої доктрини максимально вагомого значення гострим під час російської агресії, що тепер триває у форматі повномасштабного вторгнення, замаху на анексію українських територій та системної геноцидальної політики окупантів, яка супроводжується максимальним поширенням дезінформації та мови ненависті.

Автор пропонує обґрунтований висновок про тривалий та системний підхід Європейського суду з прав людини до аспектів поширення недобросовісної інформації у контексті змісту та меж дотримання прав на приватне життя, свободу слова, зібрань та інших фундаментальних прав та свобод.

Констатується, що вимір інформаційної війни у практиці Європейського суду з прав людини відображений у конструюванні цим органом системи стандартів правомірного впливу на права людини у контексті потреб демократичного суспільства та правової держави, при тому що прецедентна практика Суду не є зафіксованим набором догм, але постійно еволюціонує та демонструє потребу реагування на виклики інформаційної війни із застосуванням самого духу сучасного права та із врахуванням викликів сучасності.

Автором доведено, що наявні підходи Європейського суду з прав людини до оцінки феномену інформаційної війни, мови ненависті та дезінформації постійно розширюються

та охоплюють все нові виклики та явища, які виникають у сучасних суспільних відносинах, або ж генеруються учасниками інформаційної війни. При цьому імплементація зазначених стандартів в Україні має враховувати ситуацію воєнного стану, відповідної дерогації нашої держави від конвенційних приписів та має водночас носити системний та комплексний характер.

Ключові слова: дезінформація, дискримінація, інформаційна війна, мова ненависті, приватність пропаганда, свобода слова.

Обґрунтування актуальності. Станом на сьогодні аспекти протидії пропаганді та дезінформації у її різних формах та проявах та форми управлінського й процесуального реагування на такі явища набули для вітчизняної правничої доктрини максимально вагомого значення гострим під час російської агресії, що тепер триває у форматі повномасштабного вторгнення, замаху на анексію українських територій та системної геноцидальної політики окупантів, яка супроводжується максимальним поширенням дезінформації та мови ненависті.

Україна є членом Ради Європи та безперечно вагомою є підтримка цієї організації та її інституцій, зокрема Європейського суду з прав людини (далі – ЄСПЛ) у вимірі протидії російській агресії та сприяння євроінтеграції нашої держави. Серед іншого у ЄСПЛ перебувають на розгляді тисячі справ, пов'язані з порушенням прав людини в Україні агресором, зокрема на окупованих територіях, та Суд вже схвалив низку рішень за міждержавними заявами України, пов'язаними із російською агресією. А тому не можна ігнорувати й практику ЄСПЛ, яка склалася саме у вимірі інформаційної війни.

Таким чином дослідження практики ЄСПЛ у контексті інформаційної війни, на вбачається максимально актуальним питанням для вітчизняної правової доктрини. Аналіз рішень ЄСПЛ у вимірі протидії російської агресії можна відстежити у роботах Анцупової Т.О., Бабіна Б.В., Баймуратова М.О., Громовенка К.В., Кормича Б.А., Тицької Я.О., водночас комплексного висвітлення цих питань саме у вимірі відображення протидії дезінформації, мові ненависті, підтримки російської агресії сучасні монографічні роботи українських авторів поки не пропонують.

Тому **метою** цієї статті слід вважати аналіз особливостей практики ЄСПЛ у вимірі формування європейських правових стандартів поведінки з поширенням інформації як вагомому фактору інформаційної війни, для цього слід вирішити такі наукові **завдання**, як аналіз узагальненої практики Суду стосовно поведінки з інформацією, межі правомірного впливу поширюваної інформації на приватні інтереси людини та правомірну діяльність держави, зокрема у вимірах медіа, зібрань, правоохоронної діяльності та протидії дискримінації.

Методологічно стаття виконана з використанням комплексу сучасних та традиційних методів та підходів юридичної науки, зокрема із застосуванням онтології та герменевтики, які традиційно використовуються для аналізу практики ЄСПЛ, так саме як й з застосуванням порівняльних, програмних, прогностичних, аналітичних та системних методів, які

використовувалися для висвітлення складових формування та розвитку практики Суду у вимірі поточних викликів інформаційної війни.

Під час дослідження були узагальнені рішення ЄСПЛ у їх автентичному англomовному вигляді на платформі Суду HUDOC, а також використані офіційні посібники ЄСПЛ для юристів-практиків щодо викладання базових рішень Суду за конкретними статтями Конвенції про захист прав людини і основоположних свобод та протоколів до неї (далі – Конвенція).

Виклад основного матеріалу. Вагома увага ЄСПЛ до викликів інформаційної війни простежується за низкою напрямів, зокрема у контексті протидії дискримінації. У цьому контексті ЄСПЛ розглядає расову дискримінацію як расове насильство та включає у склад цього явища й поширення відповідної інформації. Як констатує ЄСПЛ у низці рішень, зокрема «Начова та інші проти Болгарії» 2005 року, «Стоїца проти Румунії» 2008 року, «Сейдич і Фінци проти Боснії і Герцеговини» 2009 року, «Соаре та інші проти Румунії» 2011 року та інші, ганебність расової дискримінації та небезпечність її наслідків зумовлюють потребу у особливій увазі та системній реакції на прояви такої дискримінації з боку структур державної влади, зокрема й у вимірі протидії поширенню відповідної расистської пропаганди [1].

Водночас у наведених та в інших рішеннях, таких як «Д.Г. та інші проти Чеської Республіки» 2007 року, ЄСПЛ підкреслює потребу боротьби з расизмом через укріплення державою «демократичного бачення суспільства, у якому різноманіття сприймається не як загроза, а як джерело збагачення», «побудованому на принципах плюралізму та поваги до різних культур».

ЄСПЛ вимагає у наведених рішеннях та у справі «Абду проти Болгарії» 2014 року, проводити «проводити офіційне розслідування з рішучістю та неупередженістю» та покладає на владні органи окремий обов'язок «вжити всіх розумних заходів для встановлення існування расистських мотивів, а також визначити, чи відіграли роль у подіях почуття ненависті або упередження» та констатує «необхідність постійно підтверджувати суспільне засудження расизму та етнічної ненависті» та водночас підтримувати впевненість вразливих міноритарних груп у спроможності публічної влади захищати меншини від будь-якої загрози насильства на ґрунті расової упередженості, ненависті та пропаганди [1].

При цьому таке розслідування, як вказує ЄСПЛ у рішеннях в справах «Менсон та інші проти Сполученого Королівства» 2003 року та «Шкорянець проти Хорватії» 2017 року, не має обмежуватися власне фабулою кримінального провадження та носити ширші правомірні форми, аніж ординарне процесуальне реагування [1], цей підхід безперечно вбачається актуальним й для аспектів реагування на поширення расистських заяв у форматі пропаганди чи дезінформації.

Водночас ЄСПЛ у низці рішень у справах, таких як «Ідентоба та інша проти Грузії» 2015 року «М.К. та А.К. проти Румунії» 2016 року,

«Агдгомелашвілі та Джапарідзе проти Грузії» 2020 року, «Гендердок-М та М.Д. проти Республіки Молдова» 2021 року, «Група підтримки жіночих ініціатив та інші проти Грузії» 2021 року, вказував що обов'язок органів влади з'ясовувати дискримінаційний мотив протиправних дій не є абсолютним, але державні структури «повинні зробити все, що є розумним за даних обставин, для збору та збереження доказів, вивчення всіх практичних засобів встановлення істини та винесення повністю обґрунтованих, неупереджених та об'єктивних рішень, не оминаючи увагою підозрілі факти, які можуть свідчити про насильство, спричинене, наприклад, дискримінацією» [4].

У цьому вимірі характерним є приклад справи «Картер проти України» 2024 року, за якою ЄСПЛ у рішенні визнав, що органи Національної поліції не реагували на очевидні дискримінаційні мотиви протиправних дій проти заявника, й що це не тільки «підірвало перспективи належного розслідування ймовірного злочину, вчиненого на ґрунті ненависті», але й сформувало «байдужість, еквівалентну офіційній згоді та навіть потуранню злочинам на ґрунті ненависті» [8].

У рішеннях в справах «Сабаліч проти Хорватії» 2021 року та «Оганезова проти Вірменії» 2022 року ЄСПЛ констатував, що розслідування протиправних дій за підозрою у їх дискримінаційній природі має бути неупередженим та ретельним, серед іншого «зважаючи на необхідність постійно підтверджувати засудження суспільством таких дій». Визнаючи відсутність абсолютного зобов'язання держав щодо наявності у кожній такій справі саме обвинувального вироку, зокрема зважаючи на потребу доведеності провини та змагальності процесу, ЄСПЛ при цьому все одно вимагає, щоб національні суди не демонстрували інертність, волокиту та формалізм саме для сприяння уникнення відповідальності та щоб за умов встановлення вини покарання не носило явно формальний характер [4]; [5]. Все це має неабияке значення й для справ щодо поширення мови ненависті або дезінформації дискримінаційного характеру: прикладом суди не мають обмежуватися констатацією формальних аспектів порушення та повинні враховувати дискримінаційний зміст чи підґрунтя поширеної засудженим інформації під час призначення покарання.

Водночас ЄСПЛ встановлює й істотні вимоги до правоохоронних органів, які виявляють та розслідують злочини, пов'язані із поширенням інформації. Прикладом у рішеннях в справах «Біг Брозер Уотч проти Сполученого Королівства» 2021 року, «Екімджієв та інші проти Болгарії» 2022 року, «Центр за правосуддя проти Швеції» 2022 року, ЄСПЛ вимагав особливої ретельності під час проведення правоохоронцями «необхідних запобіжних заходів в рамках режимів масового перехоплення повідомлень» або ж «сигнальної розвідки», які проводяться насамперед для протидії ворожим пропагандистським операціям та іншим формам інформаційного впливу, з боку «іноземної розвідки та нових загроз від як відомих, так і невідомих осіб» [5].

ЄСПЛ у цьому вимірі вимагав від держав, які проводять масові перехоплення повідомлень чіткого законодавчого визначення «категорія осіб, які можуть бути піддані перехопленню їхніх комунікацій, а також природи протиправних дій, які можуть стати підставою для наказу про перехоплення» та наголосив у контексті такого масового перехоплення на «важливості нагляду та перевірки, яка посилюється через вроджений ризик зловживання та законну необхідність у таємності» [5]. Водночас ЄСПЛ, як це випливає з системи його наведених рішень, не вбачав порушення конвенційних прав у самій по собі процедурі масових перехоплень, за умов що воно здійснюється в рамках протидії істотно суспільно небезпечним та водночас визначеним та детермінованим явищам та процесам, але не у вимірі невизначеності підстав, загальної але не встановленої «ймовірності» чи «потребами у профілактиці».

Так саме ЄСПЛ, констатуючи правомірність збору та зберігання правоохоронними та контррозвідувальними органами держави великих обсягів інформації, без чого не вбачається можливим й проведення заходів протидії пропаганді, мові ненависті та інформаційним впливам, у низці рішень вказував на потребу дотримання принципу пропорційності, а також потреби у «низці гарантій проти свавілля і зловживань», які мають існувати для запобігання несанкціонованого витоку накопиченої інформації, або ж для уникнення зайвих обмежень прав людини чи соціального інтересу під час її масштабного оприлюднення владою, зокрема з процесуальною чи профілактичною метою [5].

Таку позицію, серед іншого, ЄСПЛ зайняв у справах «М.К. проти Франції» 2013 року, «Соро проти Естонії» 2015 року, «Анчев проти Болгарії» 2017 року, «Айкагуер проти Франції» 2017 року, «Медієнгруппе Остеррайх ГмбХ проти Австрії» 2022 року, серед іншого у вимірі поширень викривальної інформації про комуністичні чи нацистські прояви. ЄСПЛ особливо підкреслив, що таке поширення, як фактично форма інформаційної протидії на захист демократії, було правомірним, оскільки, прикладом, у Болгарії «процедура розголошення була суворо регламентована й супроводжувалася низкою гарантій проти свавілля і зловживань», «була доручена спеціальній незалежній комісії», акти якої можна було оскаржувати у суді з можливістю апеляції [2].

Водночас у рішеннях в справах «Зегерштедт-Віберг та інші проти Швеції» 2006 року та «Гаф'юк проти Румунії» 2020 року ЄСПЛ визнав порушення конвенційних прав заявників, які відповідно робили заяви «за насильницький опір поліцейським перевіркам під час демонстрацій» або ж на підтримку комуністичного режиму, та надалі не просто залишалися у базах даних правоохоронців, але й отримували обмеження власних прав через 20-30 років після відповідних заяв, які не призводили саме до кримінальної відповідальності, але до внесення у «профілактичні переліки» [2].

ЄСПЛ також досліджував протидію поширенню інформації у контексті зібрань, та у низці рішень визначав межу правомірного втручання

влади у відповідні процеси. Прикладом, у рішенні в справі «Діліпак проти Туреччини» 2015 року Суд встановив протиправність обмеження прав мітингарів через їх заяви, які «не закликають до насильницьких діянь чи до кривавої помсти, не виправдовують вчинення терористичних актів, не поділяють цілі прихильників терору, та не можуть бути витлумачені як вірогідне заохочення до насильства через вираження глибоко вкоріненої та ірраціональної ненависті до визначених осіб» [2].

Водночас у справах «Ферідун Язар проти Туреччини» 2004 року, «Їлмаз і Кілич проти Туреччини» 2008 року, «Їюль та інші проти Туреччини» 2010 року ЄСПЛ у власних рішеннях визнав правомірними дії влади з розгону мітингів після того як їх учасники поширювали гасла «на підтримку незаконного збройного угруповання», які «містили особливо насильницький підтекст», або ж поширювали гасла відверто насильницького характеру, «демонстрували підтримку незаконної збройної організації у публічній промові». У цих справах, визнаючи у цілому правомірність дій поліції та спецслужб Туреччини, ЄСПЛ водночас наголошував, що «загальновідомі стереотипні політичні гасла, які вигукували під час законних демонстрацій, не можна тлумачити як заклик до насильства чи повстання», водночас визнаючи що оцінка ступеня реагування та такі гасла мала врахувати «українську напружену політичну атмосферу, що панувала в країні на той час» [2].

Питання пропаганди та мови ненависті ЄСПЛ досліджував й у інших напрямках рішень, у цьому вимірі дуже вагомим та характерним вбачається рішення Суду у справі «Кіркоров проти Литви» 2024 року, у якому надавалася оцінка змісту цілей національної безпеки та громадського порядку, які були застосовані для виправдання заборон на в'їзд іноземців. Суд у справі підкреслив, що відповідному російському виконавцю і продюсеру правомірно заборонили в'їзд до Литви, оскільки зробили це не через його окремі заяви або виступи, а через проведену литовською владою цілком об'єктивну оцінку системних діянь заявника як «інструмента м'якої сили росії» [7].

ЄСПЛ у п. 61 цього рішення констатував, що він «посилається на пояснення Департаменту міграції [Литви] про те, що РФ використовувала різні засоби пропаганди, включаючи телебачення, соціальні мережі, фільми та популярних виконавців, таких як заявник, який бажав приїхати з Росії для проведення концертів, проти країн Балтії. Пропаганда була спочатку спрямована на місцеві російські громади, проте її метою також було вплинути на ширшу аудиторію – російськомовних або тих, хто прагнув «славної ери радянського союзу». Як зазначає Департамент, заявник не заперечував, що він був інструментом «м'якої сили» РФ, а фізична присутність заявника в Литві була необхідною для поширення дезінформації та пропаганди РФ» [7], а тому заборона на в'їзд у Литву була правомірною та прав заявника не порушила.

Висновки. Отже, слід констатувати тривалість та системність підходу ЄСПЛ до аспектів поширення недобросовісної інформації у контексті змісту та меж дотримання прав на приватне життя, свободу слова, зібрань

та інших фундаментальних прав та свобод. Вимір інформаційної війни у практиці ЄСПЛ відображений у конструюванні цим органом системи стандартів правомірного впливу на права людини у контексті потреб демократичного суспільства та правової держави, при тому що прецедентна практика Суду не є зафіксованим набором догм, але постійно еволюціонує та демонструє потребу реагування на виклики інформаційної війни із застосуванням самого духу сучасного права та із врахуванням викликів сучасності.

Наявні підходи ЄСПЛ до оцінки феномену інформаційної війни, мови ненависті та дезінформації постійно розширюються та охоплюють все нові виклики та явища, які виникають у сучасних суспільних відносинах, або ж генеруються учасниками інформаційної війни. При цьому імплементація зазначених стандартів в Україні має враховувати ситуацію воєнного стану, відповідної дерогації нашої держави від конвенційних приписів та має водночас носити системний та комплексний характер, що зумовлює гостру потребу подальших наукових досліджень викликів інформаційної війни у описаному вище контексті.

Література:

1. Заборона дискримінації. Посібник зі статті 14 Європейської конвенції з прав людини та статті 1 Протоколу № 12 до Конвенції. ЄСПЛ-KS. URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_14_art_1_protocol_12_ukr
2. Захист даних. Посібник із судової практики Європейського суду з прав людини. Оновлено 31 серпня 2024 року. ЄСПЛ-KS. URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_data_protection_ukr
3. Масові протести. Посібник із судової практики Європейської конвенції з прав людини. Оновлено 31 серпня 2024 року. ЄСПЛ-KS. URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_mass_protests_ukr
4. Права ЛГБТІ. Посібник із судової практики Європейської конвенції з прав людини. Оновлено 31 серпня 2024 року. ЄСПЛ-KS. URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_rights_of_lgbti_persons_ukr
5. Право на повагу до приватного і сімейного життя, житла і кореспонденції. Посібник зі статті 8 Європейської конвенції з прав людини. Оновлено 31 серпня 2024 року. ЄСПЛ-KS. URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_ukr
6. Свобода вираження поглядів. Посібник зі статті 10 Європейської конвенції з прав людини. Оновлено 31 серпня 2024 року. ЄСПЛ-KS. URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_10_ukr
7. Filip Bedros Kirkorov against Lithuania, 12174/22. Decision 19.III.2024 [Section II]. HUDOC. URL: <https://hudoc.echr.coe.int/fre?i=001-233417>
8. Karter V. Ukraine, 18179/17. Judgment 11.4.2024 [Section V]. HUDOC. URL: <https://hudoc.echr.coe.int/eng?i=002-14305>

Kushnir V. Practice of European Court of Human Rights as Factor of Informational Warfare

Summary. In the article, the author analyzes the peculiarities of the practice of the European

Court of Human Rights in the dimension of the formation of European legal standards for dealing with the dissemination of information as a significant factor in information warfare. For this purpose, an analysis of the generalized practice of the Court regarding the handling of information, the limits of the legitimate influence of disseminated information on the private interests of a person and the legitimate activities of the state, in particular in the dimensions of the media, assemblies, law enforcement activities and combating discrimination was conducted.

The author emphasizes in the article that as of today, the aspects of countering propaganda and disinformation in its various forms and manifestations and the forms of managerial and procedural response to such phenomena have acquired the greatest importance for the domestic legal doctrine, acute during the Russian aggression, which is now continuing in the format of a full-scale invasion, an attempt to annex Ukrainian territory and the systemic genocidal policy of the occupiers, which is accompanied by the maximum spread of disinformation and hate speech.

The author offers a reasoned conclusion about the long-term and systematic approach of the European Court of Human Rights to the aspects of the dissemination of unfair information in the context of the content and limits of observance of the rights to privacy, freedom of speech, assembly and other fundamental rights and freedoms.

It is stated that the dimension of information warfare in the practice of the European Court of Human Rights is reflected in the construction by this body of a system of standards of legitimate influence on human rights in the context of the needs of a democratic society and a state governed by law, while the case law of the Court is not a fixed set of dogmas, but is constantly evolving and demonstrates the need to respond to the challenges of information warfare using the very spirit of modern law and taking into account the challenges of modernity.

The author proves that the existing approaches of the European Court of Human Rights to the assessment of the phenomenon of information warfare, hate speech and disinformation are constantly expanding and covering all new challenges and phenomena that arise in modern social relations, or are generated by participants in information warfare. At the same time, the implementation of these standards in Ukraine must take into account the situation of martial law, the corresponding derogation of our state from the convention provisions, and must at the same time be systemic and comprehensive.

Key words: discrimination, disinformation, freedom of speech, hate speech, information warfare, privacy, propaganda.



Стаття надійшла до редакції 18.10.2025

Стаття прийнята 24.10.2025

Статтю опубліковано 17.11.2025

МІЖНАРОДНЕ ЕКОЛОГІЧНЕ ПРАВО

УДК 343.97
DOI <https://doi.org/10.32782/ILA.2025.34.02>

МАМЕДОВ Р. А.

аспірант кафедри морського та міжнародного права
Карпатського національного університету імені Василя Стефаника
ORCID: 0009-0001-8636-7756

ДИРЕКТИВИ ЄВРОПЕЙСЬКОГО СОЮЗУ У СФЕРІ ПРОТИДІЇ КРИМІНАЛЬНИМ ПРАВопорушенням ПРОТИ ДОВКІЛЛЯ

Анотація. Вказана стаття присвячена комплексному аналізу проблем протидії кримінальним правопорушенням проти довкілля у Європейському Союзі, а також дослідженню основних шляхів ефективної імплементації європейських підходів у національне законодавство України. У праці серед іншого розглядаються основні напрями європейської політики у сфері охорони навколишнього природного середовища, а також ключові інституції Європейського Союзу, які здійснюють координацію та реалізацію політики у сфері охорони довкілля і політики у сфері кримінальної юстиції. Особливу увагу у статті приділено аналізу новоприйнятої Директиви (ЄС) 2024/1203 «Про захист довкілля за допомогою кримінального права», яка визначає оновлені підходи до криміналізації діянь, які завдають шкоди навколишньому природному середовищу, а також встановлює єдині стандарти відповідальності держав-членів Європейського Союзу у даній сфері. Також, у статті проведено порівняльний аналіз положень зазначеної Директиви та норм чинного Кримінального кодексу України, виокремлено основні розбіжності у підходах визначення складів кримінальних правопорушень проти довкілля, їх кваліфікуючих ознак, а також системи санкцій. Поміж іншим, також зроблено акцент на тому факті, що чинний Кримінальний кодекс України не охоплює значну кількість діянь, визначених кримінально-караними новою Директивою. З огляду на це, наголошено, що українське кримінальне законодавство потребує подальшого вдосконалення з урахуванням сучасних європейських тенденцій у галузі права у сфері охорони довкілля. Відтак, на підставі проведеного дослідження зроблено висновок про доцільність та необхідність оперативної імплементації положень Директиви 2024/1203 у національне законодавство України. Це сприятиме гармонізації правової системи нашої держави з правом Європейського Союзу, посиленню інституційної спроможності правоохоронних органів у сфері боротьби з кримінальними правопорушеннями проти довкілля, підвищенню рівня екологічної безпеки, а також забезпеченню більш ефективної реалізації євроінтеграційного курсу України.

Ключові слова: охорона довкілля, кримінальні правопорушення проти довкілля, законодавство ЄС, Директиви ЄС, протидія кримінальним правопорушенням проти довкілля, національна стратегія протидії кримінальним правопорушенням проти довкілля.

Проблеми. Протидія кримінальним правопорушенням проти довкілля є одним із пріоритетних напрямів кримінально-правової політики Європейського Союзу. Питанню збереження навколишнього природного середовища в цілому присвячені окремі розділи чи не всіх основоположних документів про організацію, створення та функціонування Європейських Співтовариств.

З часу отримання незалежності 1991 року, наша держава взяла цілеспрямований курс на Євроінтеграцію та зобов'язалася відповідно до ратифікованих міжнародних договорів та внутрішньодержавних нормативно-правових актів якнайшвидше здійснити адаптацію національного законодавства до законодавства Європейського Союзу. Частину таких зобов'язань Україна вже виконала, а частина ще потребує належного опрацювання та невідкладного впровадження до практичної реалізації.

Нині, не дивлячись на суттєву протягом останніх років активізацію діяльності щодо апроксимації законодавства України у сфері охорони довкілля до законодавства ЄС, що полягає у прийнятті численних законів та підзаконних нормативно-правових актів, недостатньо опрацьованим все ще залишається питання імплементації законодавства ЄС у сфері протидії кримінальним правопорушенням проти довкілля кримінально-правовими засобами.

Аналіз досліджень і публікацій. Окремі аспекти питань протидії ЄС кримінальним правопорушенням в цілому, та кримінальним правопорушенням проти довкілля зокрема, досліджувалися такими вітчизняними науковцями як Ю.С. Шемшученко, К.П. Задоя, А.М. Шульга, М.І. Хавронюк, В.О. Навроцький, І.І. Митрофанов, Ю.А. Турлова, Ю. В. Баулін, О.О. Житний та інші. Натомість, питанню протидії ЄС кримінальним правопорушенням проти довкілля, особливо у світлі новоприйнятої Директиви (ЄС) 2024/1203, науковцями увага фактично не приділялась.

Отже, стаття має на меті здійснити аналіз кримінального законодавства ЄС у сфері охорони довкілля, зокрема через призму новоприйнятої Директиви (ЄС) 2024/1203, що безумовно матиме суттєве значення для практичної діяльності щодо імплементації законодавства ЄС у сфері протидії кримінальним правопорушенням проти довкілля у національне законодавство України.

Виклад основного матеріалу. Протидія кримінальним правопорушенням проти довкілля є важливою складовою державної політики, адже без належної протидії злочинним діям у цій сфері, не можливо забезпечити сприятливе для існування та життєдіяльності людини та інших організмів навколишнє середовище.

Як зазначає І.В. Козич, у широкому розумінні протидія злочинності – це будь-яка діяльність у сфері соціального управління, яка, не переслідуючи спеціальної мети, сприяє зменшенню злочинності, у тому числі шляхом забезпечення верховенства права та реалізації його інших принципів. У той же час, у вузькому розумінні протидія злочинності – це система

заходів політичного, правового, організаційно-управлінського, ідеологічного, соціального та іншого характеру, спрямованих на зниження злочинності, усунення її чинників, виявлення, припинення та розслідування злочинів, притягнення винних до юридичної відповідальності, відновлення законних прав та інтересів фізичних і юридичних осіб. [1, с. 23]

Питанням охорони довкілля пронизані установчі акти Європейського Союзу. Так, у Преамбулі Консолідованої версії Договору про ЄС однією з цілей утворення цього Співтовариства закріплено, зокрема, принципи сталого розвитку та формування внутрішнього ринку на засадах захисту навколишнього середовища. Розділ XX Договору має назву «Довкілля», в якому визначено досягнення таких цілей: збереження, захист та поліпшення якості довкілля; захист здоров'я людей; раціональне використання природних ресурсів; сприяння на міжнародному рівні у вирішенні регіональних і світових проблем довкілля, захист клімату. [2, с. 1-2]

У свою чергу, правове регулювання питань, що стосуються навколишнього середовища, в державах-членах здійснюється за допомогою норм національного, європейського та міжнародного права, однак із верховенством європейського права, що виявляється в наданні нормам останнього вищої юридичної сили. [3, с. 508]

Охорона довкілля, а також протидія кримінальним правопорушенням проти довкілля в ЄС забезпечується системою діючих нормативно-правових актів (джерелами права ЄС), а також Інституціями (органами), які покликані забезпечувати виконання цих нормативно-правових актів. При цьому, подібно як нормативно-правові акти існують на загальноєвропейському та національному рівнях держав-членів ЄС, аналогічно на загальноєвропейському та національному рівнях діють й відповідні Інституції.

До основних органів, які регулюють питання політики ЄС у сфері охорони довкілля відносяться: Рада ЄС, Європейський Парламент, Європейська Комісія, Генеральний директорат з питань навколишнього середовища, Генеральний директорат з питань клімату, Генеральний директорат з питань сільського господарства та розвитку сільських районів, Європейське агенство навколишнього середовища (ЕЕА), Комітет регіонів тощо.

Крім того, серед інституцій кримінально-правової політики ЄС можна виділити: Європейський Парламент, Європейську Раду, Раду (Раду Міністрів), (Європейську) Комісію, Суд Правосуддя Європейського Союзу, Європейський Центральний Банк, Суд (Палата) Аудиторів, Комітет Європейського парламенту з громадянських свобод, правосуддя та внутрішніх справ – European Parliament Committee on Civil Liberties, Justice and Home Affairs, Тимчасові комітети з вирішення конкретних проблем. [4, с. 11]

Джерела права охорони навколишнього середовища ЄС – це зовнішнє вираження правових норм, що діють у межах ЄС і регулюють суспільні відносини з питань охорони навколишнього середовища. Вони включають норми первинного права, норми вторинного права, прецедентне право та міжнародні договори. Первинне право становлять норми, закріплені

в установчих договорах та договорах, що їх доповнюють, на основі яких діють Європейський Союз та Європейські Співтовариства. Вони мають вищу юридичну силу, пряму дію на території держав-членів Європейського Союзу, є безпосереднім джерелом прав і обов'язків його суб'єктів. Таким чином, норми первинного права закріплені у двох установчих договорах: Договорі про функціонування Європейського Союзу (до вступу в силу Лісабонського договору іменувався Договором про заснування Європейського Співтовариства або Римським договором, діє з 1958 року) і Договорі про Європейський Союз (Маастрихтський договір, діє з 1993 року), які в поєднанні утворюють правові основи ЄС та відповідно права охорони навколишнього середовища ЄС. У свою чергу, до норм вторинного права ЄС, які приймаються на основі установчих договорів, належать директиви, регламенти, рішення, рекомендації та висновки. Право охорони навколишнього середовища ЄС в основному ґрунтується на директивах, що є нормативно-правовими актами Європейського Союзу, які закріплюють правила загального характеру, мають юридично обов'язкову силу і є обов'язковими для виконання на території всього Європейського Союзу. Директиви спрямовані на забезпечення гармонізації національного права, введення спільного правового регулювання в конкретних сферах суспільного життя. Держави-члени зобов'язані інкорпорувати норми, передбачені директивою у своє національне законодавство, тим не менш є вільними у виборі засобів для їх досягнення та можуть самостійно обирати форми і методи дій. Якщо державною-членом не буде приведено законодавство у відповідність із директивою протягом вказаного періоду часу, це буде вважатися порушенням зобов'язань відповідно до установчого договору і тягне за собою відповідні дії з боку Європейської Комісії. [3, с. 513-515]

Основними Директивами, що донедавна регулювали питання кримінально-правової охорони навколишнього середовища ЄС були Директива 2008/99/ЄС від 19.11.2008 «Про кримінально-правову охорону довкілля» [5] та Директива 2009/123/ЄС від 21.10.2009 про внесення змін до Директиви 2005/35/ЄС «Про забруднення з суден та про запровадження штрафів за порушення». [6]

Однак, 11.04.2024 прийнято нову Директиву (ЄС) 2024/1203 Європейського Парламенту та Ради про захист довкілля за допомогою кримінального права та про заміну Директив 2008/99/ЄС та 2009/123/ЄС. [8]

Порівнювати попередні та діючі Директиви у цілях даної статті не має необхідності, оскільки чинне законодавство України у даній сфері не проходило вагомих процедур апроксимації до зазначених вище Директив. Відтак, з практичної точки зору імплементації підлягатимуть положення вже нової Директиви 2024/1203.

Так, не дивлячись на те, що дана Директива не є обов'язковою для нашої держави, її положення містять базові фундаментальні принципи та інструменти, які безумовно підвищать ефективність протидії кримінальним правопорушенням проти довкілля у нашій державі.

Як приклад, Директива декларує необхідність розробити та опублікувати національну Стратегію протидії кримінальним правопорушенням проти довкілля, яка має переглядатися щонайменше кожні 5 років та має містити: 1) цілі та пріоритети національної політики у сфері кримінальних правопорушень проти довкілля, а також механізми регулярної оцінки їх досягнення; 2) повноваження та обов'язки усіх компетентних органів, залучених до боротьби з кримінальними правопорушеннями проти довкілля, питання координації та співпраці між ними; 3) питання щодо підтримання спеціалізації відповідних фахівців у правоохоронних органах, оцінки ресурсів, виділених на боротьбу з кримінальними правопорушеннями даної категорії, а також визначення їх майбутніх потреб.

Принагідно варто згадати, що як на доктринальному, так і на законодавчому рівнях, у нашій державі відсутня належна доктрина та стратегія протидії кримінальним правопорушенням не тільки проти довкілля, а й кримінальним правопорушенням в цілому.

Крім того, вказана Директива містить ряд практичних інструментів, які, вважаю, мають бути невідкладно імplementовані в національне законодавство нашої країни.

Так, дана Директива визначає наступний перелік кримінальних правопорушень проти довкілля: 1) скидання, викид або введення певної кількості матеріалів чи речовин, енергії чи іонізуючого випромінювання в повітря, ґрунт чи воду, що спричиняє або може спричинити смерть або серйозне каліцтво будь-якої особи, або суттєву шкоду якості повітря, ґрунту чи води, або суттєву шкоду екосистемі, тваринам чи рослинам; 2) розміщення на ринку з порушенням заборони або іншої вимоги, спрямованої на захист навколишнього середовища, продукту, використання якого у великих масштабах, а саме використання продукту кількома користувачами, незалежно від їхньої кількості, призводить до викиду, випромінювання або введення певної кількості матеріалів або речовин, енергії або іонізуючого випромінювання в повітря, ґрунт або воду та спричиняє або може спричинити смерть або серйозне каліцтво будь-якої особи або суттєву шкоду якості повітря, ґрунту або води, або суттєву шкоду екосистемі, тваринам або рослинам; 3) виробництво, розміщення або надання на ринку, експорт або використання речовин, як таких, так і в сумішах або у виробах, включаючи їх включення до складу виробів, якщо така поведінка спричиняє або може спричинити смерть або серйозну травму будь-якої особи, суттєву шкоду якості повітря, ґрунту або води, або суттєву шкоду екосистемі, тваринам або рослинам, та: а) обмежена відповідно до Розділу VIII та Додатку XVII до Регламенту (ЄС) № 1907/2006 Європейського Парламенту та Ради; б) заборонена відповідно до Розділу VII Регламенту (ЄС) № 1907/2006; в) не відповідає Регламенту (ЄС) № 1107/2009 Європейського Парламенту та Ради; г) не відповідає Регламенту (ЄС) № 528/2012 Європейського Парламенту та Ради; ґ) не відповідає Регламенту (ЄС) № 1272/2008 Європейського Парламенту та Ради; д) заборонена відповідно до Додатка I до

Регламенту (ЄС) 2019/1021 Європейського Парламенту та Ради; 4) виробництво, використання, зберігання, імпорту або експорту ртуті, сполук ртуті, сумішей ртуті та продуктів з додаванням ртуті, якщо така поведінка не відповідає вимогам, викладеним у Регламенті (ЄС) 2017/852 Європейського Парламенту та Ради та спричиняє або може спричинити смерть або серйозні травми будь-якої особи, суттєву шкоду якості повітря, ґрунту чи води, суттєву шкоду екосистемі, тваринам чи рослинам; 5) виконання проєктів у значенні статті 1 (2) (а), як зазначено у статті 4 (1) та (2) Директиви 2011/92/ЄС Європейського Парламенту та Ради, якщо такі дії здійснюються без дозволу на забудову та завдаються або можуть завдати суттєвої шкоди якості повітря та ґрунту, або якості чи стану води, або суттєвої шкоди екосистемі, тваринам чи рослинам; 6) збір, транспортування або обробка відходів, нагляд за такими операціями та подальший догляд за місцями захоронення, включаючи дії, що вживаються як дилер або брокер, якщо така поведінка: а) стосується небезпечних відходів, яка визначено у статті 3 (2) Директиви 2008/98/ЄС Європейського Парламенту та Ради та стосується значної кількості таких відходів; б) стосується відходів, відмінних від тих, що зазначені в пункті (і), та спричиняє або може спричинити смерть або серйозне каліцтво будь-якої особи, або суттєву шкоду якості повітря, ґрунту чи води, або суттєву шкоду екосистемі, тваринам чи рослинам; 7) перевезення відходів у значенні пункту (26) статі 3 Регламенту (ЄС) 2024/1157 Європейського Парламенту та Ради, якщо такі дії стосуються незначної кількості, незалежно від того, чи здійснюються вони одним перевезенням, чи кількома перевезеннями, які здаються пов'язаними між собою; 8) переробка суден, що підпадають під дію Регламенту (ЄС) № 1257/2013, якщо така поведінка не відповідає вимогам, зазначеним у пункті (а) статі 6 (2) зазначеного Регламенту; 9) скидання забруднюючих речовин з суден, що підпадають під дію статті 3 Директиви 2005/35/ЄС, у будь-яку зону, зазначено у статті 3 (1) цієї Директиви, за винятком випадків, коли таке скидання з суден відповідає умовам для винятків, викладених у статті 5 цієї Директиви, що спричиняє або може спричинити погіршення якості води або шкоду морському середовищу; 10) експлуатація або закриття об'єкта, на якому здійснюється небезпечна діяльність, або на якому зберігаються чи використовуються небезпечні речовини чи суміші, якщо така поведінка та така небезпечна діяльність, речовина чи суміш підпадають під дію Директиви 2012/18/ЄС Європейського Парламенту та Ради або Директиви 2010/75/ЄС Європейського Парламенту та Ради, і така поведінка спричиняє або може спричинити смерть або серйозне каліцтво будь-якої особи, або суттєву шкоду якості повітря, ґрунту чи води, або суттєву шкоду екосистемі, тваринам чи рослинам; 11) будівництво, експлуатація та демонтаж установки, якщо така поведінка та така установка підпадають під дію Директиви 2013/30/ЄС Європейського Парламенту та Ради, і така поведінка спричиняє або може спричинити смерть або серйозні травми будь-якої особи, або суттєву шкоду якості повітря, ґрунту чи води, або

суттєву шкоду екосистемі, тваринам чи рослинам; 12) виробництво, переробка, обробка, використання, утримання, зберігання, транспортування, імпорт, експорт або утилізація радіоактивного матеріалу чи радіоактивних речовин, якщо така поведінка та такий матеріал чи речовини підпадають під дію Директиви Ради 2013/59/Євратом, 2014/87/Євратом або 2013/51/Євратом, і така поведінка спричиняє або може спричинити смерть або серйозні травми будь-якої особи або суттєву шкоду якості повітря, ґрунту чи води, або суттєву шкоду екосистемі, тваринам чи рослинам; 13) забір поверхневих або підземних вод у значенні Директиви 2000/60/ЄС Європейського Парламенту та Ради, якщо така поведінка завдає або може завдати суттєвої шкоди стану довкілля чи екологічному потенціалу поверхневих водних об'єктів або кількісному стану підземних водних об'єктів; 14) вбивство, знищення, вилучення, заволодіння, продаж або пропонування на продаж зразка або зразків виду дикої фауни чи флори, перелічених у Додатку IV або в Додатку V, якщо види в цьому Додатку підлягають тим самим заходам, що й ті, що прийняті для видів у Додатку IV до Директиви Ради 92/43/ЄЕС та зразка або зразків видів, зазначених у статті 1 Директиви 2009/147/ЄС Європейського Парламенту та Ради, за винятком випадків, коли такі дії стосуються незначної кількості таких зразків; 15) торгівля зразком або зразками, або їх частинами чи похідними, видів дикої фауни чи флори, перелічених у додатках А та В до Регламенту Ради (ЄС) № 338/97, та імпорт зразка або зразків, або їх частин, чи похідних, таких видів, перелічених у додатку С до зазначеного Регламенту, за винятком випадків, коли така поведінка стосується незначної кількості таких зразків; 16) розміщення або надання на ринку Союзу чи експорт з ринку Союзу відповідних товарів чи відповідних продуктів з порушенням заборони, встановленої статтею 3 Регламенту (ЄС) 2023/1115, за винятком випадків, коли така поведінка стосується незначної кількості; 17) будь-яка поведінка, яка спричиняє погіршення стану середовища існування в межах охоронюваної території або порушення видів тварин, перелічених у пункті (а) Додатка II до Директиви 92/43/ЄЕС, в межах охоронюваної території, у значенні статті 6 (2) цієї Директиви, якщо таке погіршення або порушення є значним; 18) ввезення на територію Союзу, розміщення на ринку, утримання, розведення, транспортування, використання, обмін, дозвіл на розмноження, вирощування або культивування, випускання в навколишнє середовище або поширення інвазійних чужорідних видів, що викликають занепокоєння Союзу, якщо така поведінка порушує: а) обмеження, викладені у статті 7 (1) Регламенту (ЄС) № 1143/2014 Європейського Парламенту та Ради, та спричиняє або може спричинити смерть або серйозне каліцтво будь-якої особи, або суттєву шкоду якості повітря, ґрунту чи води, або суттєву шкоду екосистемі, тваринам чи рослинам; б) умова дозволу, виданого відповідно до статті 8 Регламенту (ЄС) № 1143/2014, або авторизації, наданої відповідно до статті 9 зазначеного Регламенту, чи спричиняє або може спричинити смерть або серйозні травми будь-якої особи, або суттєву

шкоду якості повітря, ґрунту чи води, або суттєву шкоду екосистемі, тваринам чи рослинам; 19) виробництво, розміщення на ринку, імпорту, експорту, використання або викид речовин, що руйнують озоновий шар, окремо або у вигляді сумішей, як зазначено у статті 2, пункті (а) Регламенту (ЄС) 2024/590 Європейського Парламенту та Ради, або виробництво, розміщення на ринку, імпорту, експорту або використання продуктів та обладнання, а також їх частин, що містять речовини, що руйнують озоновий шар, або функціонування яких залежить від цих речовин, як зазначено у статті 2 (b) зазначеного Регламенту; 20) виробництво, розміщення на ринку, імпорту, експорту, використання або випуск фторованих парникових газів, окремо чи у вигляді сумішей, як зазначено у статті 2, пункті (а) Регламенту (ЄС) 2024/573 Європейського Парламенту та Ради, або виробництво, розміщення на ринку, імпорту, експорту або використання продуктів та обладнання, а також їх частин, що містять фторовані парникові гази або функціонування яких залежить від цих газів, як зазначено у статті 2, пункті (b) зазначеного Регламенту, або введення в експлуатацію таких продуктів та обладнання [7, с. 66-68]. Крім того, Директива передбачає можливість для держав-членів передбачати додаткові кримінальні правопорушення з метою захисту довкілля (стаття 3). [8]

З наведеного переліку діянь, які Директива відносить до кримінально-караних, вбачається, що більшість із передбачених Директивою норм є бланкетними та відсилають до відповідних профільних Директив, що регулюють ту чи іншу сфері охорони навколишнього середовища. Такий спосіб законодавчого регулювання проблеми протидії кримінальним правопорушенням проти довкілля є досить цікавим для дослідження та застосування. Крім того, порівнюючи перелік злочинних діянь згідно Директиви та чинного Кримінального кодексу України, слушно приходимо до висновку про обмеженість та абстрактний характер статей КК України. Так, для прикладу, більшість з наведених в Директиві діянь прямо не охоплюються жодною статтею чинного КК України, а за деякі з них відповідальність передбачена лише опосередковано чи частково.

Також, досліджувана Директива визначає критерії «суттєвої шкоди» довкіллю, серед яких: базовий стан ураженого навколишнього середовища, довготривалість шкоди, масштаб та оборотність пошкодження, а також критерії визначення «чи може поведінка завдати шкоди якості повітря, води або ґрунту, екосистемі, тваринам чи рослинам»: поведінка стосується діяльності, яка вважається ризикованою або небезпечною для довкілля чи здоров'я людини, та вимагає дозволу, який не був отриманий або не виконаний; ступінь перевищення нормативного порогу, значення або іншого обов'язкового параметра, встановленого законодавством або дозволом; характеристика матеріалу або речовини як небезпечної, вибухонебезпечної чи шкідливої для довкілля або здоров'я людини.

Для використання у національній практиці також важливо звернути увагу на види основних та додаткових покарань за вчинення кримінальних

правопорушень проти довкілля у світлі досліджуваної Директиви. Вказаний перелік санкцій є значно ширшим, аніж визначений чинним КК України, який містить застарілі, характерні скоріше «поліцейській», аніж «демократичній» країні, види основних та додаткових покарань за вчинення злочинів цієї категорії, серед яких: штраф, громадські роботи, пробаційний нагляд, обмеження та позбавлення волі, заборона обіймати посади та займатися певною діяльністю (використовується як основне і додаткове покарання) [9].

Так, Директива містить такі пропорційні та ефективні санкції, не передбачені чинним КК України, як: 1) зобов'язання відновити навколишнє середовище протягом певного періоду, якщо пошкодження є оборотним, або виплатити компенсацію за шкоду, завдану довкіллю, якщо шкода є незворотною або правопорушник не в змозі здійснити таке відновлення; 2) позбавлення доступу до державного фінансування, включаючи тендерні процедури, гранти, концесії та ліцензії; 3) анулювання дозволів та уповноважень на здійснення діяльності, що призвела до відповідного кримінального правопорушення; 4) тимчасова заборона балотуватися на державні посади; 5) за наявності суспільного інтересу, після оцінки кожної окремої справи, публікація всього судового рішення або його частини, що стосується скоєного кримінального правопорушення, та призначених покарань чи заходів, які можуть містити персональні дані засуджених осіб. [8]

Аналогічно, особливі види додаткових покарань встановлено Директивою й для юридичних осіб, причетних до скоєння такого виду правопорушень.

Також, Директива декларує необхідність при призначенні покарань враховувати обтяжуючі та пом'якшуючі обставини.

Серед обтяжуючих обставин Директива виділяє: 1) правопорушення спричинило руйнування екосистеми або незворотну чи довготривалу суттєву шкоду; 2) правопорушення скоєно злочинною організацією; 3) правопорушення вчинене шляхом використання підроблених документів; 4) правопорушення скоєно службовою особою державного органу під час виконання службових обов'язків; 5) правопорушник раніше був засуджений за вчинення аналогічного кримінального правопорушення; 6) правопорушення призвело або могло призвести до отримання суттєвих фінансових вигод або дозволило уникнути суттєвих витрат; 7) правопорушник знищив докази або залякав свідків чи заявників; 8) правопорушення скоєно у межах території, класифікованої як зона спеціальної охорони. Серед пом'якшуючих обставин Директива виділяє такі: 1) правопорушник відновив довкілля до його попереднього стану або до початку кримінального провадження мінімізував вплив та масштаби шкоди чи усунув завдану шкоду; 2) правопорушник надав (надає) компетентним органам інформацію, яку вони інакше не змогли б отримати, допомагаючи їм: ідентифікувати докази або притягнути до відповідальності інших порушників; знайти докази. [8]

Крім того, Директивою встановлено мінімальні строки притягнення осіб до кримінальної відповідальності за вчинення правопорушень проти довкілля (за правопорушення, яке передбачає покарання у виді позбавлення волі на строк до 10 років – щонайменше 10 років, до 5 років позбавлення волі – щонайменше 5 років тощо).

Також, Директива звертає увагу на необхідності проведення належної роботи з профілактики кримінальних правопорушень зазначеної категорії. Звертається увага на необхідності забезпечення достатньої кількості кваліфікованих кадрів в органах, що займаються виявленням, розслідуванням, а також винесенням рішень у справах про кримінальні правопорушення цієї категорії, необхідність їх належного фінансового та технічного забезпечення, проведення навчання суддів, прокурорів та працівників поліції, які здійснюють діяльність на означеному напрямку.

Висновки. Наведені вище положення Директиви (ЄС) 2024/1203, не дивлячись на те, що вона не є на даний час обов'язковою для виконання Україною, є ефективними та дієвими, зможуть забезпечити належну протидію кримінальним правопорушенням проти довкілля.

Відтак, для покращення ефективності боротьби зі злочинними діяннями у сфері охорони навколишнього середовища, необхідно щонайменше розробити національну Стратегію протидії кримінальним правопорушенням проти довкілля, яка міститиме описані вище вимоги, визначені Директивою, здійснити імплементацію повного переліку норм Директиви щодо діянь, які слід відносити до кримінальних правопорушень проти довкілля, а також передбачити національним законодавством повний спектр санкцій, передбачених цією Директивою.

Вказане має суттєве значення не тільки для забезпечення ефективної протидії кримінальним правопорушенням проти довкілля на теренах нашої держави, а й для належної інтеграції нашої держави до Європейської Спільноти та завершення виконання взятих на себе зобов'язань щодо адаптації національного законодавства України до Європейських Стандартів.

Література:

1. Козич І.В. Кримінально-правова політика в сфері протидії злочинам, що вчиняються з застосуванням насильства/дисертація на здобуття наукового ступеня кандидата юридичних наук/ Львів, 2012, 214 с.
2. Костицький В.В. (Вестмінстерська фундація за демократію). Система законодавства ЄС у сфері охорони довкілля, її основні відмінності від екологічного законодавства України/Дослідження 1. Екологічне право ЄС та його порівняння з українським екологічним законодавством. URL: <https://internews.ua/storage/app/media/rang/Materials/2024/EU/EUEcology1.pdf> (дата посилання 08.09.2025), 57 с.
3. Екологічне право: підручник/ [А.П. Гетьман, Г.В. Анісімова, А.К. Соколова та ін.]; за ред. А.П. Гетьмана, Харків, Право, 2021, 552 с.
4. Основи кримінальної політики Європейського Союзу/ початковий посібник/ автори-упорядники: О.О. Житний, Г.С. Рибалко, Д.С. Слінько, Харків, 2022, 147 с.

5. Директива 2008/99/ЄС про кримінально-правову охорону довкілля, інтернет-ресурс. URL: <https://compass27.info/dyrektyva-2008-99-yes-pro-kryminalno-pravovu-ohoronu-dovkillya/> (дата звернення 08.09.2025).
6. Directive 2009/123/EC of the European Parliament and the Council of 21 October 2009 amending Directive 2005/35/EC on the ship-source pollution and on the introduction of penalties for infringements (Text with EEA relevance), інтернет-ресурс. URL: <https://eur-lex.europa.eu/eli/dir/2009/123/oj/eng> (дата звернення 08.09.2025).
7. Логвинський Г.В., Інвестиційні інтереси та право екологічної безпеки ЄС: Кримінально-правовий підхід, *Держава та регіони*, серія Право, 2024 № 1 (83), с. 64–69. DOI: <https://doi.org/10.32782/1813-338X-2024.1.9>.
8. Consolidated text: Directive (EU) 2024/1203 of the European Parliament and of the Council of 11 April 2024 on the protection of the environment through criminal law and replacing Directives 2008/99/EC and 2009/123/EC, інтернет-ресурс. URL: <https://eur-lex.europa.eu/eli/dir/2024/1203> (дата звернення 08.09.2025).
9. Кримінальний кодекс України, інтернет ресурс, URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення 08.09.2025).

Mamedov R. European Union Directives in the field of combating environmental crime

Summary. The article is devoted to a comprehensive analysis of the problems of combating environmental crimes in the European Union, as well as the study of the main ways of effectively implementing European approaches into the national legislation of Ukraine. The work, among other things, examines the main directions of European environmental policy, as well as key institutions of the European Union that coordinate and implement environmental and criminal law policies. The article pays special attention to the analysis of the newly adopted Directive (EU) 2024/1203 “On the protection of the Environment through Criminal law”, which defines updated approaches to the criminalization of acts that cause harm to the environment, and also establishes uniform standards of liability of the Member States of the European Union in this area. The article also conducts a comparative analysis of the provisions of the said Directive and the norms of the current Criminal Code of Ukraine, identifying the main differences in approaches to determining the elements of criminal offenses against the environment, their qualifying features, as well as the system of sanctions. Among other things, it was also emphasized that current Criminal Code of Ukraine does not cover a significant number of acts defined as criminally punishable by the new Directive. In view of this, it was emphasized that Ukrainian criminal legislation requires further improvement, taking into account modern European trends in environmental law. Therefore, based on the research conducted, a conclusion was made on the feasibility and necessity of the earliest possible implementation of the provisions of Directive 2024/1203 into the national legislation of Ukraine. This will contribute to the harmonization of the legal system of our state with the law of the European Union, strengthening the institutional capacity of law enforcement agencies in the field of combating criminal offenses against the environment, increasing the level of environmental safety, and ensuring more effective implementation of Ukraine’s European integration course.

Key words: environmental protection, environmental crimes, EU legislation, EU Directives, combating environmental crimes, national strategy for combating environmental crimes.

Стаття надійшла до редакції 05.10.2025

Стаття прийнята 25.10.2025

Статтю опубліковано 17.11.2025



МІЖНАРОДНЕ МОРСЬКЕ ПРАВО

УДК 341:347.8

DOI <https://doi.org/10.32782/ILA.2025.34.03>

БОРЩЕВСЬКА О. М.

кандидат юридичних наук, доцент,

доцент кафедри національного та міжнародного права

Одеського національного морського університету

ORCID: 0000-0003-2549-429X

КІБЕРНЕТИЧНА БЕЗПЕКА СУДНОПЛАВСТВА: МІЖНАРОДНО-ПРАВОВИЙ ТА НАЦІОНАЛЬНО-ПРАВОВИЙ АСПЕКТИ

Анотація. Актуалізація тематики кібернетичної безпеки судноплавства в її міжнародно-правовому та національно-правовому аспектах обумовлюється прогресом цифровізації майже всіх галузей життя людства. Цифровізація життя, в тому числі і судноплавства, створила певні прогресивні можливості з одного боку, а з іншого боку спровокувала певний ризик кіберризиків. Морські судна як автономні так і з екіпажем курсують як окремі кіберматеріальні системи, які є дуже вразливими як до зовнішніх матеріальних факторів, так і до нематеріальних факторів, зокрема, кібератак. Особливу значущість це питання набуває на сучасному етапі не тільки в умовах глобальної торгівлі, а й в умовах війни в Україні та інших світових збройних конфліктах, як елемент міжнародної та національної безпеки, яка включає повний перелік від воєнної та державної безпеки до екологічної безпеки, в тому числі на глобальному рівні.

Всеохоплююче впровадження діджитал технологій зумовлює виникнення відповідних відносин, які мають регулюватися правовими нормами, оскільки неврегульованість законодавством такого глобального сегменту технологій може мати тенденцію до вчинення дій, які будуть навмисно чи через недбалість порушувати права інших осіб.

Сучасні приклади кібератак ставлять під загрозу функціонування багатьох електронних реєстрів, доступу до баз даних, дистанційне управління процесами, зокрема повітряними та морськими суднами. Особливо це стосується забезпечення діяльності автономних суден.

У статті розглядається позиція міжнародної спільноти щодо забезпечення кібербезпеки у судноплаванні. Проаналізовано міжнародно-правову базу, стандарти та керівні документи, що регулюють кіберризик на морі. Наведено огляд національного нормативно-правового матеріалу, який імплементує або має імплементувати відповідні міжнародні норми. Порушено питання доцільності надання таким нормам імперативного (обов'язкового) характеру з метою досягнення регуляторної ефективності. Визначено, що впровадження міжнародних стандартів та норм з кібербезпеки у судноплавному секторі є критично важливим стратегічним

елементом інтеграції України у міжнародну спільноту. Запропоновано розробку та прийняття систематизованого національного нормативно-правового акта, який би забезпечив комплексне дотримання вимог кібербезпеки у судноплаванні.

Виокремлене питання дотримання національної, в тому числі, й екологічної безпеки через дотримання правил кібербезпеки. Оцінено необхідність створення спеціальної програми підготовки фахівців з кібербезпеки саме для судноплавства у вищих навчальних закладах.

Ключові слова: національна безпека, безпека судноплавства, кібербезпека, кіберінцидент, кібератака, кіберризик, судно, порти, екологічна безпека.

Постановка проблеми. Наразі через важелі економічної вигоди та подекуди, безпеки членів екіпажу, якщо йдеться про прохід судна через небезпечні ділянки морів та океанів, дуже активно розвивається електронавігація, технології щодо безпеки та зв'язку на судні, автоматизація процесів керування судном.

Слід зазначити, що судові системи та програми оновлюються під час здійснення рейсу судна через відкритий доступ до мережі Інтернету і це викликає ряд питань щодо забезпечення безпечної експлуатації судна.

Стан дослідження. Оскільки тематика досить нова то інноваційними дослідженнями в правовому полі з питань кібербезпеки займалося не таке велике коло вчених, але серед небагатьох слід зазначити наукові напрацювання В.Г. Пядишева, В.С. Веремчука, Б.М. Орловського, які аналізують міжнародний досвід організації кібербезпеки на борту суден в розрізі міжнародно-правових механізмів, які стосуються кібербезпеки мореплавства, але на жаль, не надають певних правових рекомендацій щодо закріплення технічних норм щодо кібербезпеки як загальнообов'язкового правила поведінки, що має певний механізм державного примусу та відповідно переведення таких норм у нормативно-правове закріплення з відповідними імперативами виконання.

Мета статті – дослідити позицію міжнародної спільноти щодо забезпечення кібербезпеки в судноплаванні та привести національний нормативно-правовий матеріал з цієї тематики у відповідність до міжнародних норм. При цьому визначити доцільність надання таким нормам імперативного характеру.

Визначити необхідність імплементації міжнародних норм та стандартів щодо кібербезпеки у судноплаванні як важливий стратегічний елемент інтеграції України в міжнародне співтовариство.

Надати пропозиції щодо розробки та прийняття систематизованого національного нормативно-правового акту щодо дотримання кібернетичної безпеки в судноплаванні.

Оцінити необхідність спеціальної підготовки фахівців з кібернетичної безпеки саме у судноплаванні в закладах вищої освіти.

Виклад основного матеріалу. Загальновідомо, що будь-які відносини для ефективного їх здійснення мають бути врегульовані на рівні законодавства з раціональним механізмом правового регулювання. Тому, метою статті є аналіз міжнародного законодавства у порівнянні з законодавством

України для визначення шляхів унормування існуючих рекомендаційних та технічних норм в систему імперативних нормативних актів, а також визначення кола відносин, які мають бути закріплені на рівні законодавства щодо кібербезпеки, зокрема в судноплаванні, з подальшим формуванням відповідної підгалузі морського права.

В цьому зв'язку слід звернути увагу, що дуже слушно зазначає В.М. Веремчук про те, що морську кібербезпеку доцільно вважати відносно новою підгалуззю міжнародного морського права, яка набуває все більшого значення у зв'язку із безперервною цифровізацією морської галузі, широким використанням автоматизованих систем управління на борту суден та зростаючою кількістю кіберзагроз [1, с.61]

Поряд з цим слід зауважити, що кібербезпека судна має визначатися як сукупність правових, організаційних, технічних та операційно-програмних заходів, що спрямовані на забезпечення стійкого, безпечного та безперервного функціонування всіх систем судна, що повинно включати запобігання несанкціонованому доступу до інформації, її знищенню, спотворенню тощо.

Кібербезпека на теперішній час стала невід'ємним елементом загальної системи забезпечення безпеки судна, зокрема, та судноплавання взагалі. Від забезпечення належного рівня кібербезпеки залежить недопущення чи вчасне виявлення кіберінцидентів, що можуть спричинити загрозу життю та здоров'ю екіпажу, безпеці судна, вантажу, в окремих випадках господарській діяльності власника судна, а також екологічній безпеці на морі.

З огляду на певне перспективне бачення кіберзагроз можна визначити окремі інциденти, які з розвитком глобалізації цифрових технологій, можуть, на жаль, розширяти коло таких правопорушень, а саме:

- фальсифікація чи інше втручання в картографічну інформацію, яка знаходиться в електронному вигляді;
- несанкціоноване оновлення програмного забезпечення через втручання кіберпіратів, що призводить до збоїв у процесі технічного обслуговування;
- знищення або спотворення даних з систем глобального навігаційного супутникового зв'язку.

Але, виходячи з того, що ІМО (Міжнародна морська організація) відносить лише наступні системи судна до найбільш вразливих судових систем, з боку суб'єктів кібератак, зокрема, системи ходового містка; системи обробки та управління вантажем; системи управління двигунами, машинами та енергоживленням; системи контролю доступу на судно; системи обслуговування пасажирів та екіпажу; публічні інтернет-мережі судна, призначені для використання пасажирями; адміністративні системи та мережі; системи зв'язку [2], можна говорити про те, що поза увагою залишаються певні опції щодо логістичних систем та портів.

Тому, з огляду на вищезазначене слід визнати, що кібербезпека судноплавання має становити вже не лише комплексний правовий інститут,

а виділятися в окрему підгалузь права, яка буде охоплювати регламентацію заходів із виявлення, попередження, реагування та усунення наслідків кіберзагроз, які спрямовуються на суднові інформаційні та навігаційні системи через інциденти, що впливають на доступність, цілісність або достовірність даних необхідних для повноцінного функціонування та життєдіяльності судна та екіпажу.

Через вищезазначене предмет правового регулювання підгалузі кібербезпеки судноплавства можна визначити як сукупність суспільних відносин, що пов'язані із правовим, організаційним, технічним та операційно-програмним заходами захисту суден, портів, логістичних та навігаційних шляхів та систем від кіберзагроз, які встановлюють відповідальність за кіберінциденти у судноплавстві через нанесення шкоди чи загрозу життю та здоров'ю екіпажу, безпеці судна, вантажу, в окремих випадках господарській діяльності власника судна, а також екологічній безпеці на морі.

Слід зазначити, що в міжнародній правовій практиці вже напрацьовано ряд документів, які регламентують в правовому полі такі відносини, але такі нормативні акти зазвичай носять рекомендаційний чи описово-правовий характер і не відбивають всіх необхідних заходів, правового регулювання, які необхідні для унеможливлення, недопущення чи перешкоджання кіберінцидентів, які мають носити імперативний характер та мати відповідні санкції.

Наприклад, Резолюція MSC.428(98) «Управління кіберризиками в морській галузі у межах систем управління безпекою»[3], яка ухвалена Міжнародною морською організацією (ІМО), визначає необхідність інтеграції управління кіберризиками до існуючих систем управління безпекою суден відповідно до вимог Міжнародного кодексу управління безпекою [4]. В ній також наголошується на необхідності підвищенні рівня обізнаності персоналу судноплавних компаній і членів екіпажу щодо актуальних кіберзагроз з метою забезпечення безпеки судна та захисту морського судноплавства загалом. Членів екіпажу просто інформують про можливі загрози, але не прописують належним чином інструментарій протидії.

У межах цієї Резолюції державам-членам ІМО рекомендується після 01 січня 2021 року забезпечувати врахування кіберзагроз у системах управління безпекою суден під час першої щорічної перевірки відповідності вимогам Міжнародного кодексу управління безпекою. Можна припустити, що кібербезпека визначається дійсно як невід'ємна частина загальної безпеки судноплавства, але питання щодо подальших річних перевірок залишається відкритим, бо кіберзагрози не мають прив'язки до календарного року.

З зазначеної вище дати управління кіберризиками стало обов'язковим елементом систем управління безпекою суден через що відсутність інформації про кіберризики в документації може бути визначена як порушення вимог Міжнародного кодексу управління безпекою, що тягне адміністративну відповідальність, яка передбачає навіть заборону виходу судна з порту.

ІМО рекомендує Посібник з кібербезпеки на борту суден [5], в якому визначається коло потенційних суб'єктів кібератак, а саме, активісти, включаючи незадоволених працівників; злочинні угруповання; опортуністи; держави та державні утворення; терористичні організації. Як бачиться з контексту цієї рекомендації, це мають бути потенційні суб'єкти, на яких слід звертати увагу, бо коло суб'єктів, які можуть спричинити кіберінциденти має бути визначено більш ширшим, оскільки це можуть бути будь-які особи, які є незадоволеним працівником, опортуністом тощо, а також можуть бути найманою особою, яка працює за гроші чи за іншу користь.

Цікавими є циркуляри MSC.1/Circ.1639 від 14 червня 2021 та MSC-FAL.1/Circ.3/Rev.3 від 04 квітня 2025 року Комітету з безпеки на морі Міжнародної морської організації, які носять також лише рекомендаційний характер, де державам-членам пропонується взяти до уваги рекомендації, що містяться у четвертій версії «Керівництва з кібербезпеки на суднах», яка підготовлена галузевими асоціаціями. В ньому рекомендується відповідним заінтересованим сторонам, включаючи судновласників, операторів та менеджерів, враховувати при необхідності цей посібник при розгляді кіберризиків на суднах відповідно до цілей та функціональних вимог Міжнародного кодексу управління безпекою, як це рекомендовано Резолюцією MSC.428(98) [6]. Наразі, в сучасних умовах, які існують у світі необхідно визначити імперативний характер таких норм, тобто не рекомендувати, а запровадити на нормативному рівні оцінку відповідності системи управління безпекою судноплавства вимогам кібербезпеки.

Попри наявність на міжнародному рівні ще певної кількості нормативних актів щодо кібернетичної безпеки в судноплавстві проблема ефективного врегулювання таких правовідносин все ще залишається досить важливою. Це відбувається через, як зазначалося, по-перше, рекомендаційний характер таких нормативних актів. По-друге, можна відмітити відсутність уніфікованої Конвенції з кібербезпеки в мореплавстві, а також певну сегментарність у регулюванні цих відносин між різними міжнародними морськими організаціями. По-третє, і це може виглядати основною перешкодою, неготовність держав, логістичних компаній та судновласників до практичного впровадження імперативних вимог щодо нівелювання кіберризиків в судноплавстві, а також складнощів з обміном інформацією про кіберінциденти на міжнародному рівні.

Незважаючи на ці недоліки, система міжнародних актів створює те загальне нормативне поле, у межах якого держави можуть формувати власну політику у сфері кібербезпеки у судноплавстві.

В національному законодавстві України також існують деякі нормативні акти про кібербезпеку та кіберризики, але ці норми, по-перше, не уніфіковані, а, по-друге, не мають саме цільового спрямування щодо судноплавства.

Так, профільний закон щодо кібербезпеки Закон України «Про основні засади забезпечення кібербезпеки України» [7] окреслює лише

основні принципи, термінологію та коло державних органів, що стосується цієї галузі, але не надає ані поняття кібербезпеки, у судноплаванні як галузі національного господарства, ані окремих вимог щодо кібербезпеки для судноплавання, логістичних компаній та портів.

Якщо говорити про ширше поняття безпеки, таке як національна безпека, то в Законі України «Про національну безпеку України» [8] кібербезпеку включено в перелік складових національної безпеки, але саме в сфері судноплавання прямо не визначено. Аналогічна ситуація з законами України «Про транспорт» [9] та «Про морські порти» [10], які спрямовані лише на управління транспортною інфраструктурою та інфраструктурою портів, але про регулювання питань пов'язаних з кібербезпекою в них не йдеться.

Щодо Кодексу торговельного мореплавання України [11], то він більш орієнтований на питання безпеки навігації, охорони без врахування киберризиків та закріплює безпеку судноплавання у векторі організації морських перевезень.

Навіть Стратегія кібербезпеки України на 2021-2025 роки [12] лише визначає морську інфраструктуру критичною, містить окремі загальні позиції щодо захисту критичної інфраструктури, але будь-які спеціальні вимоги щодо кібербезпеки у судноплаванні відсутні.

З огляду на такі прогалини в законодавстві щодо неврегульованості на достатньому законодавчому рівні правовідносин з дотримання кібернетичної безпеки в судноплаванні можна констатувати відсутність і правового зобов'язання ефективно реалізовувати політику кібербезпеки в системах управління безпекою суден, зокрема, і судноплавання взагалі.

Досі залишається повністю невирішеним питання створення та функціонування Єдиного органу національної кібербезпеки судноплавання в Україні, який би консолідував моніторинг кіберінцидентів в судноплаванні та проводив політику щодо дотримання кібербезпеки саме у судноплаванні і відповідно координував би свою діяльність з Центральними органами влади України.

Так, вважається за необхідне на рівні міжнародного законодавства, яке в подальшому має бути імплементоване в українське законодавство [13] підготувати нормативний акт, який би містив методологію оцінки кіберризиків. Такі технічні норми мають бути закріплені на міжнародному рівні, а в подальшому на рівні законодавства України як загальнообов'язкове правило поведінки, що має певний механізм державного примусу.

Тобто такі рекомендації та стандарти, що розроблені профільними фахівцями з кібербезпеки мають бути включені до складу нормативно-правових актів та мати структуру норми права: гіпотезу, диспозицію та санкцію з обов'язковим підкріпленням можливості застосування державного примусу для її дотримання.

Схематично можна навести приклад структури такого нормативно-правового акту щодо дотримання кібернетичної безпеки в судноплаванні.

Розділ перший присвятити загальним вимогам організаційного управління згідно рекомендаціям MSC.428 (98), що буде закріплювати поняття кібербезпеки у судноплаванні, необхідність наявності політики компанії з кібербезпеки, яка затверджена на рівні порту приписки судна чи судноплавної компанії; включення управління кіберризиками до документованої системи управління безпекою; визначення відповідальної особи, яка має право підпису і відповідні повноваження в порту (компанії, на судні); наявність реєстрів (інвентаризації) ІТ та ОТ-систем судна з позначенням відповідної критичності та контроль за оновленням цих реєстрів, відповідний періодичний аналіз кіберризиків.

Другий розділ може закріплювати дотримання технічних аспектів ІТ та ОТ-інфраструктури, які втілюють рекомендації IACS Rec, 166 IMO Guidelines v4 [14] такі як, наявність фізичної та логічної сегментації офісної та операційної мережі; обов'язкового контролю відділеного доступу з документацією сесій; зобов'язання щодо регулярного оновлення ПЗ з фіксацією часу; запровадження резервного копіювання критичних даних на ізольованих носіях; ведення журналу безпеки із моніторингом подій кіберінцидентів; постійна перевірка антивірусного ПЗ та відповідних систем; можливість процедури фізичного контролю доступу до ІТ-обладнання серверів та мережевих шаф; наявність окремої мережі для систем навігації, енергетики та камер безпеки.

Третій розділ може містити інструкцію-план реагування на кіберінциденти з певним нормативним описом процедур ідентифікації, реагування, відновлення систем та подальшого звітування; закріплення обов'язку кожного члену екіпажу знати порядок дій у разі кібератаки; вимоги проводити навчання та моделювання вправ з реагування на кібератаки; обізнаність щодо можливості звернення до відповідного органу, якій опікується кібернетичною безпекою в судноплаванні в даному регіоні, в даній компанії чи порту приписки судна.

Четвертий розділ має регламентувати питання підготовки та обізнаності екіпажу з обов'язковою наявністю не тільки підтверджуючих документів з зовнішніх навчань, а безпосередньо ознайомлення під особисте зобов'язання з системами реагування на кіберінциденти в безпосередній зоні роботи, а також дозволи щодо користування персональними пристроями з інтернет-підключенням.

В п'ятому розділі, серед іншого, необхідно зазначити питання сертифікації та документування розслідування кіберінцидентів та аналізу їх причин, визначення суб'єктів та рівнів відповідальності за правопорушення в галузі кібербезпеки судноплавання.

А шостий розділ присвятити безпосередньо заходам правового реагування на невиконання, неналежне виконання закріплених вище вимог чи дії, які мають прямий чи непрямий умисел на настання кіберінциденту, зокрема, чи спричинення ситуації яка загрожує настанням кібернебезпеки в цілому.

І ще одну велику проблему, яка не прямо залежить від поля правового регулювання, але, на яку також слід звернути увагу для розв'язання в подальшому це відсутність українського програмного забезпечення та відповідного обладнання для розвитку захисту кіберпростору.

В зв'язку з цим, як один з напрямків розвитку та посилення кібербезпеки в судноплаванні, є досить перспективним впровадження в закладах вищої освіти освітніх програм, які б поєднували та формували спеціальні компетенції здобувачів вищої освіти для отримання ними таких результатів навчання, які б дозволили випускниками бути конкурентноспроможними на ринку професій які стосуються поглибленої спеціалізації кіберзахисту, кібербезпеки та її нормативно-правового наповнення.

Висновки. Отже, підсумовуючи вищевикладене, можна констатувати, що кібербезпека у судноплаванні є дуже важливим напрямком для розвитку і розширення, в тому числі, й в ракурсі нормативно-правового регулювання.

Якщо міжнародне законодавство, як зазначалося, перебуває в стадії бурхливого розвитку, але все одно носить рекомендаційний характер, залишаючись при цьому базою для управління кіберризиками в судноплаванні для добросовісних користувачів, то для потенційних порушників таке законодавство має носити імперативний характер.

Для нашої держави імплементація міжнародних норм та стандартів щодо кібербезпеки у судноплаванні є, поміж іншого, важливим стратегічним елементом інтеграції України в міжнародне співтовариство, що буде сприяти забезпеченню усталеності процесів як в морегосподарському комплексі в цілому, так і в судноплаванні, зокрема.

Вдається раціональною пропозиція розробки та прийняття систематизованого національного нормативно-правового акту щодо дотримання кібернетичної безпеки в судноплаванні.

Розширити коло потенційних суб'єктів кібератак, на яких слід звертати увагу, порівняно з колом, що рекомендує Посібник з кібербезпеки на борту суден, оскільки це може бути по суті будь-яка особа, яка працює за гроші чи за іншу користь.

Ініціювати створення Єдиного органу національної кібербезпеки судноплавання в Україні, який би консолідував моніторинг кіберінцидентів в судноплаванні та проводив політику щодо дотримання кібербезпеки саме у судноплаванні і відповідно координував би свою діяльність з Центральними органами влади України.

Розглянути можливість впровадження в закладах вищої освіти освітніх програм, які б поєднували та формували спеціальні компетенції здобувачів вищої освіти для отримання ними таких результатів навчання, які б дозволили випускниками бути конкурентноспроможними на ринку професій які стосуються поглибленої спеціалізації кіберзахисту, кібербезпеки та її нормативно-правового наповнення.

Література:

1. Веремчук В.С. Проблематика імплементації міжнародно-правових стандартів морської кібербезпеки у національне законодавство України. *Приватне та публічне право*. 2025. № 2. С. 61–66. URL: <https://dspace.onu.edu.ua/server/api/core/bitstreams/5ecc31a9-8525-4e3f-a8d9-fe12349a3c32/content>
2. Міжнародна морська організація. URL: <http://www.imo.org/en/OurWork/Facilitation/FALCommittee/Facilitation/FAL41-17>.
3. Резолюція MSC.428(98) «Управління кіберризиками в морській галузі у межах систем управління безпекою» від 16 липня 2017 року. URL: <https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MS428289829.pdf>
4. Міжнародний кодекс управління безпекою, прийнятий Асамблеєю ІМО від 04.11.1993 № А.741(18), імплементований в рамках регламенту Європейського Парламенту і Ради (ЄС) № 336/2006 від 15 лютого 2006 року. URL: <https://zakon.rada.gov.ua/rada/term/en-lt/15561>
5. Посібник з кібербезпеки на борту суден підготовлений галузевими організаціями, та зведеною Рекомендацією Міжнародної асоціації класифікаційних товариств (МАКО) з кіберзахисту № 166. URL: <http://www.iacs.org.uk>
6. Циркуляри MSC.1/Circ.1639 від 14 червня 2021 та MSC-FAL.1/Circ.3/Rev.3 від 04 квітня 2025 року Комітету з безпеки на морі Міжнародної морської організації. URL: <https://www.imo.org/enghttps://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MS428289829.pdf>
7. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
8. Про національну безпеку України: Закон України від 21 червня 2018 року. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
9. Про транспорт: Закон України від 10 листопада 1994 року. URL: <https://zakon.rada.gov.ua/laws/show/232/94-%D0%B2%D1%80#Text>
10. Про морські порти України: Закон України від 17 травня 2017 року. URL: <https://zakon.rada.gov.ua/laws/show/4709-17#Text>
11. Кодекс торговельного мореплавства України від 23 травня 1995 року. URL: <https://zakon.rada.gov.ua/laws/show/176/95-%D0%B2%D1%80#Text>
12. Стратегія кібербезпеки України на 2021-2025 роки, затверджена Указом Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» від 26 серпня 2021 року. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>
13. Про схвалення Стратегії імплементації положень директив та регламентів Європейського Союзу у сфері міжнародного морського та внутрішнього водного транспорту («дорожньої карти») Розпорядження Кабінету Міністрів України від 11 жовтня 2017 р. № 747-р. URL: <https://zakon.rada.gov.ua/laws/show/747-2017-%D1%80#Text>
14. Recommendation on Cyber Resilience 166, IMO Guidelines v4. URL: https://www.steamshipmutual.com/sites/default/files/downloads/articles/2020/IACS-Recommendation-on-Cyber-resilience-No-166-2020_04.pdf

Borshchevska O. Cybersecurity in shipping: international-legal and national-legal aspects

Summary. The actualization of the topic of cyber security of shipping in its international legal and national legal aspects is due to the progress of digitalization of almost all spheres of human life. The digitalization of life, including shipping, has created certain progressive opportunities on the one hand, and on the other hand has provoked a certain risk of cyber risks. Seagoing vessels, both autonomous and with a crew, operate as separate cyber-material systems that are very vulnerable to both external material factors and intangible factors, in particular, cyberattacks. This issue is gaining particular importance at the present stage not only in the context of global trade, but also in the context of the war in Ukraine and other global armed conflicts, as an element of international and national security, which includes a full range from military and state security to environmental security, including at the global level.

The comprehensive implementation of digital technologies leads to the emergence of relevant relations that should be regulated by legal norms, since the lack of regulation by law of such a global segment of technologies may tend to commit actions that will intentionally or through negligence violate the rights of other persons.

Modern examples of cyberattacks threaten the functioning of many electronic registers, access to databases, remote control of processes, in particular aircraft and sea vessels. This is especially true for ensuring the activities of autonomous vessels.

The article considers the position of the international community on ensuring cybersecurity in shipping. The international legal framework, standards and guidance documents regulating cyber risks at sea are analyzed.

An overview of national regulatory and legal material that implements or should implement relevant international norms is provided. The issue of the expediency of giving such norms an imperative (mandatory) character in order to achieve regulatory efficiency is raised. It was determined that the implementation of international standards and norms on cybersecurity in the shipping sector is a critically important strategic element of Ukraine's integration into the international community.

The development and adoption of a systematized national regulatory act is proposed, which would ensure comprehensive compliance with cybersecurity requirements in shipping. The issue of compliance with national, including environmental, security through compliance with cybersecurity rules is highlighted.

The need to create a special program for training cybersecurity specialists specifically for shipping in higher educational institutions is assessed.

Key words: national security, shipping safety, cybersecurity, cyber incident, cyber attack, cyber risk, ship, ports, environmental safety.



Стаття надійшла 203.10.2025

Стаття прийнято 24.10.2025

Статтю опубліковано 17.11.2025

ЗМІСТ

МІЖНАРОДНЕ ПРАВО ПРАВ ЛЮДИНИ

Кушнір В. В.

ПРАКТИКА ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ
ЯК ФАКТОР ІНФОРМАЦІЙНОЇ ВІЙНИ..... 3

МІЖНАРОДНЕ ЕКОЛОГІЧНЕ ПРАВО

Мамедов Р. А.

ДИРЕКТИВИ ЄВРОПЕЙСЬКОГО СОЮЗУ У СФЕРІ ПРОТИДІЇ
КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ ПРОТИ ДОВКІЛЛЯ.....11

МІЖНАРОДНЕ МОРСЬКЕ ПРАВО

Борщевська О. М.

КІБЕРНЕТИЧНА БЕЗПЕКА СУДНОПЛАВСТВА: МІЖНАРОДНО-
ПРАВОВИЙ ТА НАЦІОНАЛЬНО-ПРАВОВИЙ АСПЕКТИ..... 22

CONTENTS

INTERNATIONAL HUMAN RIGHTS LAW

Kushnir V.

PRACTICE OF EUROPEAN COURT OF HUMAN RIGHTS
AS FACTOR OF INFORMATIONAL WARFARE.....3

INTERNATIONAL ENVIRONMENTAL LAW

Mamedov R.

EUROPEAN UNION DIRECTIVES IN THE FIELD OF COMBATING
ENVIRONMENTAL CRIME.....11

INTERNATIONAL LAW OF THE SEA

Borshchevska O.

CYBERSECURITY IN SHIPPING: INTERNATIONAL-LEGAL
AND NATIONAL-LEGAL ASPECTS.....22

Здано в роботу 27.10.2025. Підписано до друку 17.11.2025.
Формат 70x100/16. Ум.-друк. арк. 2,76. Папір офсетний.
Цифровий друк. Зам. № 1225/946. Наклад 300 прим. Ціна договірна.

Видавництво і друкарня – Видавничий дім «Гельветика»

65101, м. Одеса, вул. Інглезі, 6/1

Телефон +38 (095) 934 48 28, +38 (097) 723 06 08

E-mail: mailbox@helvetica.ua

Свідоцтво суб'єкта видавничої справи

ДК № 7623 від 22.06.2022 р.