

Морська безпека як складова національної безпеки

**Матеріали круглого столу
25 жовтня 2024 року**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ОДЕСЬКА МОРСЬКА АКАДЕМІЯ
АСОЦІАЦІЯ МОРСЬКОГО ПРАВА УКРАЇНИ
КОЛЕГІЯ ЮРИСТІВ З МОРСЬКОГО ПРАВА УКРАЇНИ

***Морська безпека як складова
національної безпеки***

Матеріали круглого столу
25 жовтня 2024 року

Одеса – 2025

УДК 341.225(082)

М432

Рекомендовано до друку рішенням Вченої ради навчально-наукового інституту морського права та менеджменту Національного університету «Одеська морська академія» від 24 грудня 2024 р. (протокол № 5)

Редакційна колегія: Савінова Н.А. д.ю.н., с.н.с. (голова редколегії); Степанов С.В., к.ю.н., доцент (зам. голови редколегії); Скоробагатько А.В., д.ю.н., доцент; Ковбан А.В., к.ю.н., доцент; О.О. Ізбаш та інші.

Морська безпека як складова національної безпеки: матеріали круглого столу 25 жовтня 2024 року. – Одеса: НУОМА, 2025 – 68 с.
Укр. та англ. мовами.
ISBN 978-617-7857-43-2

У збірник увійшли матеріали круглого столу «Морська безпека як складова національної безпеки», яка відбулась в Національному університеті «Одеська морська академія» 25 жовтня 2024 р. Видання містить аналіз Морської доктрини України на період до 2035 року, проаналізовані підходи до ролі наднаціональних стандартів адміністрування морської безпеки та внутрішньодержавних механізмів її реалізації. Досліджується морська безпека як стан, який досягається за допомогою інструментів реалізації морської доктрини держави та її втілення у нормотворенні та правозастосуванні. Означено шляхи оновлення морської безпеки як складової національної безпеки України у повоєнний та мирний час.

УДК 341.225(082)

Надані учасниками матеріали надруковані із збереженням авторської редакції. Редакційна колегія не завжди поділяє думку авторів.

ISBN 978-617-7857-43-2

© Національний університет
«Одеська морська академія», 2025

ЗМІСТ

Балобанов О.О.

Повернемося до мети та загальних засад «безпеки мореплавства»..... 4

Бельо Л.Ю.

Аналіз правового регулювання національних інтересів України в сфері портових інновацій..... 7

Бондаренко К.В., Нєкрасов Д.С.

Деякі питання функціонування Морської охорони Державної прикордонної служби України в контексті прийняття Стратегії морської безпеки України 10

Валуєва Л.В.

Митна безпека та портові інновації..... 14

Допілка В.О.

Проблеми правового регулювання у морському туризмі 19

Єфтєні Н.М.

Ціннісні орієнтації українського суспільства в умовах воєнної агресії 22

Зозуля Є.В.

МВС України як суб'єкт забезпечення морської безпеки України 24

Ковбан А.В.

Національні інтереси в морській сфері: конституційно-правовий аналіз..... 28

Кузніченко О.В., Ільченко М.А.

Морська безпека, як невід'ємний компонент національної безпеки держави... 31

Литвиненко С.С.

Роль та функції міжнародних організацій у протидії тероризму на морі..... 34

Moshak Grygorii

Improvement of legal regulation of safety of navigation on waterways..... 38

Mykhailova Diana

Protecting seafarers: how warlike operations area agreements ensure safety in Black sea region..... 41

Палько В.І.

Правова політика Морської безпеки України 44

Переверзєва О.С.

Загроза морському середовищу під час воєнних дій в Україні..... 47

Пальченко А.А.

Щодо забезпечення екіпажем морських перевезень як основи національної безпеки мореплавства 50

Святюк Святослав

Основні етапи контролю судна в міжнародному морському праві 54

Скоробагатько А.В.

Дотримання трудових прав моряків – гарантія морської безпеки 57

Степанов С.В.

Аналіз міжнародного досвіду у сфері інформаційної безпеки..... 61

Сурілова А.О., Мочернюк М.О.

Взаємозв'язок тероризму та нелегальної міграції: глобальні виклики безпеки та шляхи їх подолання..... 64

трудових та соціальних прав моряків, найважливіший з яких – Конвенція про працю в морському судноплавстві. Видається очевидним, що дотримання її положень сприятиме покращенню умов праці тих хто виконує трудову функцію в морі та забезпечить їх безпеку. Допоки наша держава не ратифікує даний документ, українські моряки будуть мати обмежений обсяг правових інструментів захисту своїх трудових та соціальних прав: звернення до національних судових інстанцій, ЄСПЛ, ІМО, МОП та профспілок.

Список використаних джерел:

1. Стратегія морської безпеки України. Затверджено Указом Президента України від 17 липня 2024 р. № 468/2024 URL: <https://www.president.gov.ua/documents/4682024-51461>
2. Конвенція МОП про працю в морському судноплавстві 2006 року. URL: <https://mtu.gov.ua/files/%D0%9A%D0%BE%D0%BD%D0%B2%D0%B5%D0%BD%D1%86%D1%96%D1%8F%202006.pdf>
3. Кодекс торговельного мореплавства України від 23.05.1995 р. № 176/95-ВР. URL: <https://zakon.rada.gov.ua/laws/show/176/95-%D0%B2%D1%80>

Степанов С.В.

*кандидат юридичних наук, доцент,
доцент кафедри загальноправових дисциплін
Національного університету «Одеська морська академія»*

АНАЛІЗ МІЖНАРОДНОГО ДОСВІДУ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сьогодні, питаннями інформаційної безпеки займаються багато урядових та міжурядових організацій. Найбільш відомими серед яких є Організація з безпеки і співробітництва в Європі (ОБСЄ), НАТО та ООН.

Як відомо, перші здобутки у сфері інформатизації й телекомунікацій у контексті міжнародної безпеки з'явилися в 1998 р.

У 1998 році на засіданні Першого комітету Генеральної Асамблеї Організації об'єднаних Націй був представлений проєкт резолюції щодо інформаційної безпеки. Проєкт було ухвалено без голосування [1].

Після ухвалення проєкту була створена робоча група міжнародних експертів, які провели аналіз досягнень у сфері застосування інформаційно-телекомунікаційних технологій у контексті безпеки та визначили явні й можливі загрози світовій безпеці.

На їхнє переконання, наявні та потенційні загрози у сфері інформаційної безпеки варто віднести до найбільш серйозних проблем ХХІ сторіччя. Експерти прийшли до цього висновку у зв'язку із бурхливим розвитком науково-технологічного прогресу та впровадженням нових інформаційно-комунікаційних технологій, які у сучасному стані можуть бути спрямовані проти фізичних і юридичних осіб, національної інфраструктури та урядів. Наслідки таких загроз тісно пов'язані з усіма сферами життя, котрі становлять глобальну систему міжнародної спільноти.

Групи урядових експертів наголошували на низці рекомендацій, зокрема на необхідності продовження діалогу між суб'єктами використання ІКТ, прийняття заходів щодо обміну думками та збільшення рівня довіри між зазначеними суб'єктами, здійснення обміну інформацією стосовно національних законів і стратегій, що можуть слугувати прикладом для інших країн; створення загальної бази, спрямованої на уніфікацію норм із питань попередження й боротьби проти наявних і потенційних загроз у сфері використання інформаційних технологій.(11-13) [1][3].

Серед активних учасників можна відзначити представників Австралії, які запропонували створити в мережі Інтернет надійний кіберпростір з найвищим ступенем безпеки, який буде обслуговувати інтереси фізичних та юридичних осіб та держав.

Німеччина у своєму докладі на Генеральній Ассамблеї ООН від 2014 року наголосила на тому, що сьогодні зросли випадки «кібервійни», з боку інших держав на так звані «високоцінні» сфери, до яких відносяться об'єкти критичної інфраструктури, промисловості, крупного підприємництва, що наносить велику шкоду державному управлінню та бізнесу.

Німеччина, як економічний лідер Європейського Союзу занепокоєна питаннями кібербезпеки з 1991 року коли нею і було створено Федеральне відомство інформаційної безпеки.

У 1994 році був розроблений Інформаційний стандарт управління безпекою технологій та створені інші органи для реагування на комп'ютерні надзвичайні ситуації.

Тому в рамках свого багаторічного досвіду дослідження та боротьби з кібер-атаками вони досить вмотивовано пропонують класифікувати кіберпростір як оперативну військову область, на рівні з морським, повітряним або космічним простором, оскільки у сучасному світі кібер-інциденти можуть перерости в «реальний» конфлікт.

Для його запобігання урядом ФРН була розроблена національна стратегія боротьби з кібер-інцидентами, яка передбачає:

- Захист критичної інформаційної інфраструктури,
- Захист ІТ-систем у Німеччині,
- Посилення ІТ-безпеки в державному управлінні,
- Керування національним центром кібер-реагування,
- Створення національної ради з кібер-безпеки,
- Ефективний контроль злочинності в кібер-просторі,
- Ефективні скоординовані дії для забезпечення кібер-безпеки в Європі та

в усьому світі,

- Використовувати надійні та перевірені інформаційні технології,
- Підвищення кваліфікації кадрів у федеральних органах влади
- Розроблення інструментів реагування на кібер-атаки.[4]

Дійсно занепокоєння Німеччини є небезпідставними. Сьогодні спостерігається підвищення ролі кіберпростору у бізнесі, промисловості, приватному житті, військовій сфері, державотворенні, що може призвести до дуже непередбачуваних наслідків для всього світу.

Розуміючи це, держави, члени ООН акцентують увагу на необхідність створення мирної та безпечної інформаційної сфери, яка буде інструментом міждержавної комунікації з приводу обміну інформацією та спільній боротьбі з кібер-атаками.

В рамках цієї загрози Генеральною Асамблеєю ООН була ухвалена Резолюція 75/240 від 31 грудня 2020 року, щодо скликання нової робочої групи відкритого складу з питань безпеки у сфері використання інформаційно-комунікаційних технологій (на 2021-2025 роки) завданням якої є подальше вироблення норм, правил та принципів відповідальної поведінки держав, розгляд ініціатив держав, спрямованих на забезпечення безпеки у сфері використання ІКТ. [2]

Отже, як показує історія і практика, міждержавне співробітництво та вирішення проблем інформаційної безпеки з моменту початку у 1998 році і до сьогодні не втрачає актуальність. В рамках дослідження розробляються механізми ефективної міждержавної взаємодії задля збереження миру та безпеки у світі.

Список використаних джерел:

1. Резолюція, прийнята Генеральною асамблеєю ООН щодо Досягнень у сфері інформатизації та телекомунікації у контексті міжнародної безпеки від 4 грудня 1998 року. URL: <https://documents.un.org/doc/undoc/gen/n99/760/05/pdf/n9976005.pdf>

2. Резолюція, прийнята Генеральною асамблеєю ООН щодо Досягнень у сфері інформатизації та телекомунікації у контексті міжнародної безпеки від 31 грудня 2020 року. URL: <https://documents.un.org/doc/undoc/gen/n21/000/28/pdf/n2100028.pdf>

3. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности URL: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://digitallibrary.un.org/record/3964709/files/DSS_33_Russian.pdf%3Fln%3Des&ved=2ahUKEwiuq6yK6aeJAxVVgf0HHSrpJWsQFnoECBoQAQ&usg=AOvVaw2DMupjQuONXch0HF46mhYP

4. Звіт про розвиток у сфері інформації та телекомунікації в контексті міжнародної безпеки» (RES 68/243), Німеччина., URL: <https://s3.amazonaws.com/unoda-web/wp-content/uploads/2014/07/Germany.pdf>

Сурілова А.О.

*PhD, доцент кафедри морського права
Національний університет «Одеська морська академія»*

Мочернюк М.О.

*здобувач вищої освіти II року навчання
освітнього ступеня магістр ННІМПтаМ НУОМА
Національний університет «Одеська морська академія»*

ВЗАЄМОЗВ'ЯЗОК ТЕРОРИЗМУ ТА НЕЛЕГАЛЬНОЇ МІГРАЦІЇ: ГЛОБАЛЬНІ ВИКЛИКИ БЕЗПЕКИ ТА ШЛЯХИ ЇХ ПОДОЛАННЯ

Тероризм та незаконна міграція є одними з найгостріших проблем сучасного глобалізованого світу. Хоча ці явища мають різну природу, вони часто розглядаються у взаємозв'язку через спільні причини, наслідки та механізми протидії.

Тероризм можна розглядати як цілеспрямоване використання насильства для створення загальної атмосфери страху серед населення з метою досягнення певних політичних цілей. Сучасне терористичне насильство характеризується класичним «трикутником»: А атакує Б, щоб переконати або примусити В змінити свою позицію щодо певної дії чи політики [1].

Важливо зазначити, що визначення тероризму може суттєво варіюватися залежно від політичних, соціальних та культурних контекстів. Це призводить до неоднозначності у трактуванні тероризму на міжнародному рівні. Наприклад, у контексті Палестинсько-ізраїльського конфлікту, більшість країн і