DOI: https://doi.org/10.18524/2411-2054.2025.58.331007
УДК 341.225.5:004.056

Б. М. Орловський, докт. юрид. наук, доцент, професор
Одеський національний університет імені І. І. Мечникова
Кафедра кримінального права, кримінального процесу та криміналістики
Французький бульвар, 24/26, Одеса, 65058, Україна
e-mail: b.orlovskyi@onu.edu.ua
ORCID iD: https://orcid.org/0000-0002-9161-2904

СУЧАСНІ КІБЕРРИЗИКИ: ЇХ ПОНЯТТЯ, СТРУКТУРА ТА ЗАСТОСУВАННЯ У СФЕРІ ТОРГІВЕЛЬНОГО МОРЕПЛАВСТВА

Стаття присвячена комплексному дослідженню сучасних кіберризиків, їхнього концептуального апарату, структури та особливостей застосування у критично важливій сфері торгівельного мореплавства. У статті здійснено поглиблений аналіз сутності та змісту поняття «кіберризик», розкрито його характерні ознаки, визначено ключові джерела походження та систематизовано основні форми реалізації в контексті зростаючої цифрової залежності морської галузі.

З метою вдосконалення правового регулювання у сфері кібербезпеки, автором запропоновано власне визначення поняття «кіберризик», що інтегрує ймовірність настання негативних наслідків, наявність потенційних кіберзагроз та вразливостей інформаційних систем. Обґрунтовано доцільність законодавчого закріплення цього визначення, зокрема у профільних нормативно-правових актах, таких як Закон України «Про основні засади забезпечення кібербезпеки України» наступним чином:

«Кіберризик – існуюча ймовірність настання негативних наслідків для суб'єктів кібербезпеки, національної безпеки, суспільства та держави, що виникає внаслідок наявності потенційних кіберзагроз та/або вразливостей в інформаційних, комунікаційних та інформаційно-комунікаційних системах, а також недоліків у їх захисті, що можуть призвести до порушення конфіденційності, цілісності, доступності інформаційних ресурсів, порушення сталого та надійного функціонування зазначених систем, завдання шкоди законним інтересам фізичних та юридичних осіб, майну, критичній інфраструктурі».

У статті детально розглянуто характерні ознаки кіберризиків, серед яких виокремлено віртуальну природу їхньої реалізації, транскордонний характер поширення, динамічну еволюцію у відповідь на розвиток інформаційних технологій та потенційну масштабність негативних наслідків для різних сфер суспільного життя та національної безпеки. Особливу увагу приділено специфіці прояву цих ознак у контексті торгівельного мореплавства, де вразливість критичної інфраструктури може мати глобальні наслідки.

Проведено систематизацію джерел виникнення кіберризиків, які класифіковано на чотири основні класи: дії людей (ненавмисні помилки та навмисні зловживання), бездіяльність щодо розвитку систем та технологій (технологічні вразливості), помилки у внутрішніх процесах (організаційні недоліки) та зовнішні події (геополітичні конфлікти, дії третіх сторін, природні катастрофи). Розкрито специфіку впливу кожного з цих класів на рівень кібербезпеки у сфері морського судноплавства.

Окрему увагу приділено аналізу основних форм (інструментів) реалізації кіберризиків, до яких віднесено кібератаку, кіберінцидент, кібертероризм та кібервійну. Розглянуто їх відмінні характеристики за суб'єктивним складом, мотивацією та механізмами впливу на інформаційні системи. Підкреслено особливу вразливість торгівельного мореплавства

© Б. М. Орловський, 2025

до кожної з цих форм, з огляду на його залежність від цифрових технологій та важливість для глобальних логістичних ланцюгів.

У висновках наголошено на складності та багатогранності сучасних кіберризиків, що зумовлює необхідність комплексного правового підходу до їх регулювання з використанням міжнародно-правового досвіду. Зазначено про необхідність подальшої гармонізації чинного законодавства з міжнародними стандартами у сфері кібербезпеки для ефективної протидії кіберризикам.

Ключові слова: кіберризик, кіберінцидент, кібератака, кібертероризм, кібербезпека, торгівельне мореплавство.

Постановка проблеми. Сучасний етап розвитку суспільства характеризується стрімкою цифровізацією, яка охопила практично всі сфери людської діяльності, зокрема правові відносини, економіку, державне управління та соціальну інфраструктуру. Однак прогресивні технології призводять до появи нових викликів, серед яких особливе місце займають кіберризики – від зламування критично важливих систем до масштабних атак на персональні дані. Зростання кількості та складності кіберзагроз свідчить про недостатність ізольованих національних підходів до їх регулювання. На сьогодні багато держав, зокрема Україна, стикаються з проблемою фрагментарності законодавчої бази щодо протидії кіберзлочинності та виявлення кіберризиків, а також відсутності гармонізації з міжнародними стандартами. Між тим, кіберпростори не мають державних кордонів, і наслідки атак часто носять транснаціональний характер, що потребує уніфікованих правових механізмів запобігання та відповідальності.

Особливу загрозу становлять атаки на критичну інфраструктуру, фінансові установи, системи державного управління та об'єкти торгівельного мореплавства, які можуть призвести не лише до значних економічних втрат, а й до порушення логістичних ланцюгів, стабільності міжнародної торгівлі та суспільної безпеки. Водночас, національні законодавчі ініціативи часто відстають від динаміки розвитку кіберзлочинності, а запровадження міжнародного досвіду залишається неефективним через відсутність системного підходу.

Тому актуальність дослідження полягає в аналізі сучасних кіберризиків, виявленні прогалин у національному законодавстві щодо їх нормативного закріплення та розробці механізмів імплементації міжнародно-правових стандартів у зазначеній сфері. Важливим є визначення оптимальних шляхів використання міжнародно-правового досвіду для протидії кіберризикам у національному законодавстві, зокрема директив, рекомендацій, конвенцій, керівництв з кібербезпеки, що обумовлює необхідність подальших досліджень у цій галузі.

Аналіз останніх досліджень і публікацій показує, що дослідження кіберризиків привертало увагу різних вчених і прямо чи побічно зустрічалося у працях І. В. Арістова, В. С. Веремчука, А. О. Волошина, О. В. Гайдука, І. В. Діордіци, Є. О. Живило, В. В. Куцаєва, В. А. Ліпкана, С. Б. Майданевича, О. М. Мельника, В. Г. Пядишева, А. О. Трофименко, О. О. Тихомирова, В. П. Шеломенцева, В. С. Цимбалюка та інших. Увагу вчених привертали різні аспекти цієї тематики, по яким висловлювались власні погляди. В той же час системний розгляд цього питання залишився малодослідженим. Тому автор, спираючись на попередні дослідження, згідно із **метою цієї статті** здійснює комплексне дослідження понят-

тя та структури кіберризиків і їх впливу на сферу торгівельного мореплавства, з акцентуванням уваги на правових аспектах цієї тематики.

Відповідно до поставленої автором проблеми, завданнями дослідження стали: 1) визначення поняття «кіберризики» у чинному законодавстві та встановлення системи їх характерних ознак; 2) аналіз джерел формування кіберризиків та їх впливу на сферу торгівельного мореплавства; 3) дослідження форм (інструментів) реалізації кіберризиків та їх спрямованості на сферу торгівельного мореплавства; 4) вивчення основних джерел міжнародно-правового регулювання кіберризиків у морській сфері.

Виклад основного матеріалу. У сучасному правовому дискурсі термін «кіберризик» набуває все більшого значення через стрімку цифровізацію суспільства та зростання кіберзагроз. Проте його зміст та визначення залишаються предметом наукових дискусій, оскільки він вбирає в себе не лише технічні аспекти, а й соціальні, економічні та правові фактори. Варто розуміти що кіберризик також є правовою категорією, яка відображає потенційну можливість настання шкідливих юридичних наслідків через непрофесійну діяльність у кіберпросторі. Однак, у законодавстві України, подібно до ратифікованої «Конвенції про кіберзлочинність», відсутнє легальне визначення поняття «кіберризик». У Законі України «Про основні засади забезпечення кібербезпеки України» законодавець оперує такими термінами, як «кіберінцидент» (інцидент кібербезпеки), «кібератака», «кібершпигунство» та «кібертероризм», котрі є конкретними проявами кіберризику, проте саме поняття «кіберризик» як таке не закріплено юридично [1]. Лише на рівні підзаконних нормативно-правових актів, зокрема у «Стратегії кібербезпеки України», епізодично використовується термін «кіберризики», наприклад, у контексті «розроблення методики ідентифікації та оцінки кіберризиків» та «запровадження системи страхування від кіберризиків», однак без надання будь-якого його дефінітивного тлумачення [2]. З огляду на це, розкриття змісту поняття «кіберризик» є нагальним, оскільки воно не існує ізольовано, а формується на перетині трьох ключових вимірів: технологічного (у вигляді вразливостей інформаційних систем), соціального (через злочинні наміри суб'єктів) та правового (внаслідок недосконалості регуляторних механізмів).

На думку автора, кіберризик можливо інтерпретувати як вірогідність настання негативних наслідків в результаті реалізації кіберзагроз, що здатні завдати шкоди інформаційним системам, конфіденційності даних, фінансовій стабільності або навіть національній безпеці держави. З урахуванням цього у статті 1 «Визначення термінів» Закону України «Про основні засади забезпечення кібербезпеки України» можна було б визначити поняття «кіберризик» наступним чином:

«Кіберризик – існуюча ймовірність настання негативних наслідків для суб'єктів кібербезпеки, національної безпеки, суспільства та держави, що виникає внаслідок наявності потенційних кіберзагроз та/або вразливостей в інформаційних, комунікаційних та інформаційно-комунікаційних системах, а також недоліків у їх захисті, що можуть призвести до порушення конфіденційності, цілісності, доступності інформаційних ресурсів, порушення сталого та надійного функціонування зазначених систем, завдання шкоди законним інтересам фізичних та юридичних осіб, майну, критичній інфраструктурі».

Ознаками кіберризику виступають:

1) віртуальний характер (природа) – він проявляється та реалізується в цифровому середовищі через автоматизовані системи, що ускладнює його безпосереднє виявлення та фіксацію традиційними методами, характерними для матеріальних кримінальних правопорушень. Його існування та потенційний вплив опосередковуються функціонуванням інформаційних систем та їх даними;

2) транснаціональність (транскордонний характер) – його виникнення та поширення не обмежуються територіальними межами окремих держав. Кіберпростір за своєю суттю є глобальним, що створює складності для уніфікованого правового регулювання та міжнародного співробітництва у сфері протидії кіберзагрозам та мінімізації наслідків кіберризиків;

3) динамічність (динамічна еволюція) – його різновиди постійно еволюціонують разом із розвитком інформаційних технологій. Кіберризики характеризуються високою мінливістю та постійною адаптацією до розвитку інформаційних технологій. З появою нових технологій та методів їх використання виникають нові види кіберзагроз та, відповідно, нові форми прояву кіберризиків, що вимагає гнучкого та проактивного підходу до їхнього виявлення, оцінки та управління;

4) масштабність наслідків – за своїм впливом він може призвести до далекосяжних та каскадних негативних ефектів у різних сферах життєдіяльності суспільства та держави, включаючи економіку, державну безпеку, функціонування критичної інфраструктури, зокрема у сфері торгівельного мореплавства, а також порушення прав та законних інтересів фізичних та юридичних осіб.

Кіберризики у сфері торгівельного мореплавства, подібно до інших критично важливих галузей, характеризуються комплексною природою, що зумовлена розмаїттям факторів їх виникнення. Для цілей правового аналізу та розробки ефективних механізмів протидії, їх доцільно розподілити на чотири основні класи джерел, кожна з яких тягне за собою специфічні правові, технологічні та організаційні наслідки, що потребують окремого розгляду та врегулювання.

Перший клас джерел становлять дії людей у сфері кібербезпеки. Людський фактор є однією з найвразливіших ланок у системі кібербезпеки, особливо з точки зору необізнаності або недбалості персоналу. Ненавмисні помилки співробітників, такі як перехід за шкідливими посиланнями, відкриття інфікованих вкладень електронної пошти, використання ненадійних паролів або недотримання правил інформаційної безпеки, можуть стати причиною серйозних інцидентів. Окрему категорію становлять навмисні дії інсайдерів – співробітників, які зловживають своїм доступом до інформаційних систем з метою отримання неправомірної вигоди, шпигунства або завдання шкоди. У контексті торгівельного мореплавства дії некваліфікованого або недбалого персоналу судна чи портової інфраструктури можуть призвести до порушення роботи критично важливих систем навігації, управління вантажами або зв'язку, створюючи загрозу безпеці мореплавства та екологічній безпеці.

Другий клас охоплює бездіяльність щодо розвитку систем і технологій, яка призводить до технологічної вразливості від кіберзагроз. До цієї категорії належать вразливості програмного забезпечення та обладнання, недоліки в архітектурі інформаційних систем, відсутність своєчасних оновлень безпеки, використ-

тання застарілих технологій, а також недостатнє або неправильне налаштування засобів захисту інформації. У сфері торгівельного мореплавства залежність сучасних суден від складних комп'ютерних систем робить їх особливо вразливими до таких недоліків. В даному випадку мова йде про: а) застаріле програмне забезпечення, яке не оновлюється через відсутність нормативних вимог або економії з боку судновласників; б) відсутність стандартизованих протоколів кібербезпеки для морського транспорту, що робить судна легкою мішенню для атак; в) недосконаліть вбудованих захистів у суднових системах (навігація, двигуни, вантажний контроль), які можуть бути зламані через технічні уразливості. Невиявлені вчасно вразливості в навігаційних системах, системах управління двигуном або автоматизованих системах управління вантажами можуть бути використані зловмисниками для здійснення кібератак з метою виведення з ладу судна, зміни його курсу або викрадення цінних даних.

Третій клас джерел включає помилки у внутрішніх процесах (організаційні недоліки), які виникають через недосконаліть управлінських рішень та відсутність чітких процедур. До них зокрема відносяться: а) недостатня кіберполітика компаній, коли багато судноплавних компаній не мають чітких інструкцій з реагування на кіберінциденти; б) відсутність регулярного аудиту безпеки – деякі судна експлуатуються без перевірки їхніх цифрових систем на вразливості; в) некоректне розподілення ролей – коли, наприклад, один член екіпажу має надто широкий доступ до критичних систем. Неефективні процедури та регламенти кібербезпеки, відсутність чітких параметрів доступу до інформаційних ресурсів, неналежний контроль за дотриманням правил інформаційної безпеки, недостатнє навчання персоналу з питань кібергігієни, а також відсутність планів реагування на кіберінциденти можуть значно підвищити ризик успішної кібератаки та ускладнити ліквідацію її наслідків. У морській галузі нечітко визначені обов'язки щодо забезпечення кібербезпеки на рівні судноплавних компаній, портів та державних регуляторних органів, а також відсутність скоординованих дій у разі кіберінциденту можуть призвести до значних затримок у транспортуванні вантажів, фінансових втрат та навіть людських жертв.

Четвертий клас становлять зовнішні події такі як: а) геополітичні конфлікти, що викликають кібератаки на критичну інфраструктуру (порти, логістичні хаби) під час війн або міжнародних напружень; б) дії третіх сторін, наприклад, хакерські атаки на постачальників програмного забезпечення, яке використовується у морській галузі; в) природні катастрофи, що можуть викликати пошкодження серверів або зв'язку через стихійні лиха. В межах цього класу часто виникають цілеспрямовані кібератаки з боку зловмисних хакерських угруповань, кібертерористичних організацій або навіть держав, що здійснюються з метою шпигунства, саботажу, вимагання викупу або завдання політичної шкоди. Розвиток нових технологій, таких як штучний інтелект та квантові обчислення, може призвести до появи нових, більш складних і небезпечних видів кібератак. У контексті торгівельного мореплавства зовнішні кібератаки можуть бути спрямовані на порушення роботи портів, блокування судноплавства у стратегічно важливих регіонах, викрадення комерційної інформації або отримання контролю над суднами з метою вчинення терористичних актів. Загалом такий клас кіберризиків потребує розвитку міжнародної співпраці та створення механізмів швидкого реагування.

Для протидії джерелам розвитку кіберризиків у науці розробляються певні підходи до «керування кіберризиками», зокрема у сфері морської кібербезпеки, які включають в себе наступні складові: виявлення загроз; виявлення вразливостей; оцінка схильності до ризику; розробка заходів захисту та виявлення; розробка планів на випадок непередбачуваних обставин; реагування на кіберінциденти згідно планів та відновлення кібербезпеки [5, с. 82].

Кіберризики набувають своєї матеріалізації через різноманітні форми (інструменти) кібернетичної активності, кожна з яких має власні характеристики, мотивацію та механізми впливу на інформаційні системи. У сучасній доктрині кібербезпеки виділяють чотири ключові форми (інструменти) реалізації кіберризиків, які відрізняються за суб'єктивним складом, мотивацією та механізмом впливу на інформаційні системи: 1) кібератака; 2) кіберінцидент; 3) кібертероризм; 4) кібервійна. Особливу актуальність ця класифікація набуває у контексті торгівельного мореплавства, де кожен із зазначених інструментів може призвести до системних порушень логістичних ланцюгів.

Першою та однією з найпоширеніших форм реалізації кіберризиків є кібератака. Під кібератакою розуміється навмисна спроба порушення конфіденційності, цілісності або доступності інформаційних систем, комп'ютерних мереж або окремих пристроїв. Специфікою кібератаки є складність у встановленні конкретного часу її початку [7, с. 155]. Мотивація кібератак може бути різноманітною: від отримання несанкціонованого доступу до конфіденційної інформації з метою комерційної вигоди або шпигунства, до виведення з ладу критично важливої інфраструктури з метою завдання економічної чи політичної шкоди. Механізми кібератак також варіюються: це можуть бути вірусні атаки, DDoS-атаки (розподілені відмови в обслуговуванні), фішингові кампанії, атаки на веб-сайти тощо. У сфері торгівельного мореплавства кібератаки можуть бути спрямовані на системи управління рухом суден, навігаційні системи, портову інфраструктуру, системи зв'язку та управління вантажами, створюючи загрозу безпеці судноплавства, екологічній безпеці та економічній стабільності. Їх результатом стає: несанкціонований доступ до систем суднової навігації; блокування роботи портової інфраструктури; викрадення комерційної таємниці судноплавних компаній.

Другою важливою формою реалізації кіберризиків є кіберінцидент. Кіберінцидент визначається як будь-яка несанкціонована або непередбачена подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактору), що має фактичні або потенційні негативні наслідки для конфіденційності, цілісності або доступності інформаційних систем та даних [1]. Кіберінцидент може бути результатом як навмисних дій (кібератаки), так і ненавмисних помилок персоналу, технічних збоїв або стихійних лих. Важливою відмінністю кіберінциденту від кібератаки є відсутність обов'язкової ознаки навмисності. Наприклад, випадкове видалення важливих даних співробітником або збій у роботі програмного забезпечення, що призвів до тимчасової недоступності системи, є прикладами кіберінцидентів. У контексті торгівельного мореплавства кіберінциденти можуть призвести до втрати важливих даних про вантажі, порушення графіків руху суден, збоїв у роботі портового обладнання або проблем зі зв'язком, що, в свою чергу, може спричинити значні фінансові втрати та загрожувати безпеці море-

плавства. Кіберінцидент у сфері торгівельного мореплавства зазвичай виникає внаслідок: випадкових помилок у роботі автоматизованих систем вантажообліку; некваліфікованих дій екіпажу при експлуатації цифрових пристроїв; збоїв в роботі програмного забезпечення через відсутність своєчасних оновлень.

Третьою, особливо небезпечною формою реалізації кіберризиків є кібертероризм. Кібертероризм являє собою використання кіберпростору та інформаційних технологій для вчинення терористичних актів або підтримки терористичної діяльності [1]. Ключовою мотивацією кібертероризму є політична або ідеологічна мета, а механізми впливу спрямовані на залякування населення, дестабілізацію суспільства, завдання шкоди критичній інфраструктурі або поширення екстремістської ідеології. Кібертерористичні атаки можуть бути спрямовані на системи енергопостачання, транспортні мережі, фінансові установи, системи охорони здоров'я або урядові інформаційні ресурси. У сфері торгівельного мореплавства кібертерористичні акти можуть бути спрямовані на захоплення контролю над суднами, атаки на системи управління суден з метою створення аварійних ситуацій, блокування роботи портів чи стратегічних морських шляхів, маніпулювання даними про вантажі небезпечного характеру, порушення морських комунікацій або використання морської інфраструктури для здійснення інших терористичних атак.

Четвертою, найбільш руйнівною формою реалізації кіберризиків є кібервійна. Кібервійна визначається як збройний конфлікт у кіберпросторі між державами або їхніми уповноваженими суб'єктами. Основною мотивацією кібервійни є досягнення стратегічних військових або політичних цілей шляхом завдання значної шкоди інформаційній інфраструктурі противника. Механізми кібервійни можуть включати складні кібератаки на критично важливі об'єкти, такі як системи управління військами, енергетичні системи, транспортні мережі, фінансові системи та системи зв'язку. Кібервійна може бути як самостійним видом збройного конфлікту, так і складовою частиною традиційних військових дій. В сфері торгівельного мореплавства кібервійськові дії можуть бути спрямовані на блокування морських шляхів, знищення судноплавної інфраструктури, порушення глобальних ланцюгів постачання та завдання значних економічних збитків стороні конфлікту.

У контексті розгляду джерел та форм реалізації кіберризиків важливе значення має їх міжнародно-правове регулювання, що забезпечує однотипний підхід до їх виявлення та протидії. Наявні міжнародні інструменти, хоч і не містять повноцінної формалізованої класифікації різновидів кіберризиків, однак виділяють їх певні типи та окреслюють критично важливі сфери, що потребують захисту від кібернетичних втручань.

По-перше, треба звернути увагу на «Керівництво з управління морськими кіберризиками» ІМО (2022), яке виділяє певні зовнішні та внутрішні чинники кіберризиків та ідентифікує ключові області підвищеної вразливості на морських суднах. У керівництві наводиться визначення морського кіберризику як міри, до якої технологічний актив може бути під загрозою через певну потенційну обставину або подію, що може призвести до збоїв (несправностей) у роботі судна або безпеки судноплавства через ушкодження та втрату даних (інформації) або систем управління судном [3, с. 15]. Керівництво включає ризики, пов'язані з

порушенням працездатності систем управління ходовим містком, що безпосередньо впливає на безпеку навігації. Також до сфери уваги потрапляють системи обробки та управління вантажем, де кібератаки можуть призвести до значних економічних збитків та порушення логістичних ланцюгів. Крім того, керівництво наголошує на важливості захисту систем управління загальним рухом судна та силовою установкою, оскільки їхнє несанкціоноване втручання може мати катастрофічні наслідки. Не залишаються поза увагою і системи контролю доступу екіпажу та пасажирів, вразливість яких може бути використана для вчинення інших злочинів.

По-друге, існує «Керівництво з кібербезпеки на борту суден» (далі – Керівництво), розроблене міжнародними об'єднаннями судноплавних компаній (ICS), страховиків морського транспорту (IUMI), судновласників (BIMCO), нафтових компаній (OCIMF, INTERTANKO), вантажоперевізників (INTERCARGO), компаній з управління суднами (InterManager) тощо. Воно містить переважно технічні стандарти, що сприятимуть аналізу кібернетичних загроз та підтримці кібердисципліни на борту суден [4, с. 452].

Згідно з зазначеним Керівництвом, до переліку суб'єктів кібернетичних нападів у морській сфері належать: активісти (серед яких можуть бути і незадоволені службовці порту або судна); злочинці та злочинні угруповання; опортуністи, тобто особи, що використовують сприятливі обставини; держави та підтримувані ними структури; терористи [6, с. 184]. Тому основними завданнями Керівництва є формування рекомендацій для покращення безпеки моряків, суден, вантажів та екосистеми (навколишнього середовища), що спрямовані на допомогу в розробці належної стратегії управління кіберризиками, згідно з існуючими правилами та сучасною морською практикою. Такі рекомендації узгоджуються з діючими нормами та досвідом у сфері торгівельного мореплавства, приділяючи особливу увагу операційним процедурам, технічному оснащенню, підготовці персоналу, реагуванню на нештатні ситуації та відновленню функціональності.

Наприклад, у даний час на кожному сучасному морському судні, з метою забезпечення безпечної навігації під час кібернетичних ризиків та атак протягом рейсу, передбачено достатньо дублюючих навігаційних пристроїв на ходовому містку, навігаційних інструментів, а також належні кваліфікаційні вимоги до судноводійського складу. Крім того, на підставі міжнародних рекомендацій розробляються спеціальні інструкції щодо встановлення допустимих відхилень параметрів руху судна під час кібернетичних атак з метою гарантування безпеки його подальшого плавання [7, с. 155, 157].

Висновки і пропозиції. Підсумовуючи проведене дослідження, слід зазначити, що сучасні кіберризики являють собою складне та багатогранне явище, що вимагає комплексного правового осмислення. Запропоноване авторське визначення поняття «кіберризику», інтегруючи поняття ймовірності негативних наслідків, потенційних кіберзагроз та вразливостей інформаційних систем, є важливим кроком для його законодавчого закріплення, наприклад, у ст. 1 «Визначення термінів» Закону України «Про основні засади забезпечення кібербезпеки України». Виокремлені ознаки кіберризиків, такі як віртуальний та транскордонний характер, динамічна еволюція та масштабність наслідків, підкреслюють їх специфіку та необхідність адекватних правових механізмів реагування на них.

Окрім того, у статті систематизовано джерела виникнення кіберризиків та їхні основні форми реалізації, що є важливим для розуміння механізмів їхньої дії. Впровадження чіткого визначення поняття «кіберризику» на законодавчому рівні сприятиме підвищенню ефективності національної системи кібербезпеки та гармонізації національного законодавства з міжнародними стандартами у цій сфері.

Список використаної літератури

1. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 05.10.2017 р. Відомості Верховної Ради України. 2017. № 45. Стор. 42. Ст. 403.
2. Стратегія кібербезпеки України: затверджена Указом Президента України від 26 серпня 2021 р. № 447/2021. Офіційний вісник України. 2021. № 70. Стор. 42. Ст. 4417.
3. Веремчук В. С. Міжнародно-правове регулювання кібербезпеки у морській галузі: сучасний стан та перспективи розвитку. Вісник Одеського національного університету. Серія: Правознавство. 2024. № 38. С. 12-17.
4. Веремчук В. С. Міжнародно-правові аспекти захисту інформації на морському транспорті / Цілі сталого розвитку в аспекті зміцнення національного та міжнародного правопорядку: тези доповідей Міжнар. наук.-практ. конф. (Запоріжжя-Львів-Одеса-Ужгород-Харків-Чернівці, 27 жовт. 2023 р.). Харків: ХНУ ім. В. Н. Каразіна, 2023. С. 450-453.
5. Пядишев В. Г. Питання вдосконалення кібербезпеки морського транспорту: зарубіжний досвід. Морська безпека та оборона. 2023. № 1. С. 78-86.
6. Трофименко А. О., Майданевич С. Б., Войченко Т. О., Дорофєєва З. Я. Деякі проблемні питання впровадження стандартів кібербезпеки на морському транспорті. Водний транспорт. 2023. № 37. С. 179-188.
7. Шумілов Д. Оцінка точності визначення місця судна при обсерваційному зчисленні і параметрів маневрування при кібернетичних ризиках. International Science Journal of Engineering & Agriculture. 2024. № 3 (6). С. 154-172.

References

1. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy № 2163-VIII vid 05.10.2017. *Vidomosti Verkhovnoi Rady Ukrainy*. 2017. № 45. Stor. 42. St. 403 [in Ukrainian].
2. Stratehiya kiberbezpeky Ukrainy: zatverdzhena Ukazom Prezydenta Ukrainy № 447/2021 vid 26.08.2021. *Ofitsiinyi visnyk Ukrainy*. 2021. № 70. Stor. 42. St. 4417 [in Ukrainian].
3. Veremchuk V. S. (2024). Mizhnarodno-pravove rehuliuvannia kiberbezpeky u morskii haluzi: suchasnyi stan ta perspektyvy rozvytku. *Visnyk Odeskoho natsionalnoho universytetu. Seriia: Pravoznavstvo*, 38, 12-17 [in Ukrainian].
4. Veremchuk V. S. (2023). Mizhnarodno-pravovi aspekty zakhystu informatsii na morskomu transporti. Tsili staloho rozvytku v aspekti zmitsnennia natsionalnoho ta mizhnarodnoho pravoporiadku: tezy dopovidei Mizhnar. nauk.-prakt. konf. (Zaporizhzhia-Lviv-Odesa-Uzhhorod-Kharkiv-Chernivtsi, 27 zhovt. 2023). Kharkiv: KhNU im. V. N. Karazina, 450-453 [in Ukrainian].
5. Piadyshev V. H. (2023). Pytannia vdoskonalennia kiberbezpeky morskoho transportu: zarubizhnyi dosvid. Morska bezpeka ta oborona, 1, 78-86 [in Ukrainian].
6. Trofimenko A. O., Maidanevych S. B., Voichenko T. O., Dorofieieva Z. Ya. (2023). Deiaki problemni pytannia vprovadzhennia standartiv kiberbezpeky na morskomu transporti. Vodnyi transport, 37, 179-188 [in Ukrainian].
7. Shumilov D. (2024). Otsinka tochnosti vyznachennia mistsia sudna pry observatsiinomu zchyslenni i parametriv manevruvannia pry kibernetychnykh ryzykakh. International Science Journal of Engineering & Agriculture, 3(6), 154-172 [in Ukrainian].

Стаття надійшла 21.04.2025 р.

B. M. Orlovskyi, Doctor of Juridical Sciences, Associate Professor, Professor
Odesa I. I. Mechnikov National University
the Department of Criminal Law, Criminal Procedure and Criminalistics
24/26 Frantsuzkyi Blvd, Odesa, 65058, Ukraine
e-mail: b.orlovskyi@onu.edu.ua
ORCID iD: https://orcid.org/0000-0002-9161-2904

MODERN CYBER RISKS: THEIR CONCEPT, STRUCTURE AND APPLICATION IN THE FIELD OF COMMERCIAL SHIPPING

Summary

This article presents a comprehensive study of modern cyber risks, their conceptual framework, structure and specific manifestations in the critically important domain of commercial shipping. The research provides an in-depth analysis of the essence and substantive content of the "cyber risk" concept, elucidates its characteristic features, identifies key sources of origin, and systematizes primary forms of implementation within the context of increasing digital dependence in the maritime sector.

To enhance legal regulation in cybersecurity, the author proposes an original definition of "cyber risk" that integrates: 1) the probability of negative consequences; 2) the existence of potential cyber threats; 3) vulnerabilities in information systems. The article substantiates the rationale for incorporating this definition into relevant legal instruments, particularly the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine", as follows:

"Cyber risk means the existing probability of negative consequences for cybersecurity subjects, national security, society and the state, arising from potential cyber threats and/or vulnerabilities in information, communication and information-communication systems, as well as deficiencies in their protection, which may lead to breaches of confidentiality, integrity and availability of information resources, disruption of stable and reliable functioning of said systems, and damage to legitimate interests of individuals and legal entities, property or critical infrastructure".

The article examines in detail the characteristic features of cyber risks, including: their virtual nature of implementation; transnational spread; dynamic evolution in response to information technology development; and potential large-scale negative consequences for various spheres of social life and national security. Particular attention is devoted to the specific manifestation of these characteristics in commercial shipping, where vulnerabilities in critical infrastructure may produce global repercussions.

The research systematizes sources of cyber risks into four principal categories: 1) human actions (unintentional errors and deliberate misuse); 2) systemic and technological inertia (technological vulnerabilities); 3) internal process failures (organizational deficiencies); 4) external events (geopolitical conflicts, third-party actions, natural disasters). The specific impact of each category on maritime cybersecurity is thoroughly analyzed.

Special consideration is given to the analysis of primary forms (instruments) of cyber risk realization, including cyber attacks, cyber incidents, cyber terrorism and cyber warfare. Their distinctive characteristics are examined in terms of: a) subject composition; b) motivation; c) mechanisms of impact on information systems. The particular vulnerability of commercial shipping to each form is emphasized, given its dependence on digital technologies and importance for global supply chains.

The conclusions highlight the complexity and multifaceted nature of modern cyber risks, necessitating a comprehensive legal approach to their regulation that incorporates international legal experience. The need for further harmonization of current legislation with international cybersecurity standards to effectively counter cyber risks is emphasized.

Keywords: cyber risk, cyber incident, cyber attack, cyber terrorism, cybersecurity, commercial shipping.