DOI: https://doi.org/10.18524/2411-2054.2025.57.325403
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

І. А. Осадча, адвокат, старший викладач
Одеський національний технологічний університет
Кафедра філософії і права
вул. Канатна, 112, Одеса, 65039, Україна
e-mail: pravnic@ukr.net
ORCID iD: https://orcid.org/0000-0002-9243-1064

КРИМІНОЛОГІЧНИЙ АНАЛІЗ КІБЕРЗАГРОЗ ТА ЇХ ВПЛИВ НА ТОРГІВЕЛЬНЕ МОРЕПЛАВСТВО

Стаття присвячена кримінологічному дослідженню кіберзагроз та їх впливу на кібербезпеку у сфері торгівельного мореплавства, що є важливим та актуальним питанням для формування системи заходів щодо її запобігання та профілактики. Кіберзагроза – це сукупність негативних чинників, факторів або явищ, що за напрямком свого впливу спрямовані на пошкодження інформаційних, телекомунікаційних та інших систем, які забезпечують належне функціонування діяльності підприємств, установ, організацій або держави та захист інформації у таких системах. Кіберзагроза посягає на кібербезпеку, якою охоплюється стан повної захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі.

Авторами було виділено складові елементи кіберзагроз у сфері торгівельного мореплавства, які включають в себе технічні аспекти роботи автоматизованих систем судна та портової інфраструктури, вразливості програмного забезпечення, людський фактор та соціальну інженерію, що пов'язані з помилками користувачів, які погано розбираються у інформаційних технологіях. Проаналізовано міжнародно-правове регулювання кіберзагроз, що охоплюється «Міжнародним кодексом з охорони суден і портових засобів» (ISPS Code), «Керівництвом з управління морськими кіберризиками» (ухваленим Комітетом з безпеки на морі Міжнародної морської організації ІМО), «Керівництвом (Рекомендаціями) з кібербезпеки на борту суден» тощо.

На сьогоднішньому етапі кіберзагрози досить сильно поширені у сфері торгівельного мореплавства, оскільки: по-перше ця сфера є вельми прибутковою за своїм економічним потенціалом, та, по-друге, тісно переплетена з цифровими технологіями. Сучасні судна – це фактично плаваючі комп'ютерні системи, де автоматизовані процеси керують рухом, навігацією, енергопостачанням тощо, забезпечують зберігання та захист даних.

Авторами розглянуто детермінанти та мотивацію кіберзлочинців у цій сфері (фінансовий аспект, усунення конкурентів, мотиви помсти, ідеологічні мотиви) та сформульовано ключові заходи задля профілактики та запобігання кіберзагроз у сфері торгівельного мореплавства, які включають у себе:

- підвищення обізнаності та кіберкультури серед персоналу морських компаній, портових служб та інших учасників галузі;

- розробку та впровадження сучасних технічних засобів захисту (систем виявлення вторгнень, криптозахист паролів, мережевих екранів) у суднові системи, портову інфраструктуру та логістичні мережі;

- розробку та дотримання міжнародних стандартів і нормативних актів ІМО у сфері кібербезпеки, міжнародної співпраці та обміну інформацією;

- створення системи оперативного реагування на кіберзагрози та кіберінциденти (ідентифікація та аналіз загрози; ізоляція ураженої системи для запобігання поширення атаки; блокування шкідливого програмного забезпечення та відновлення роботи системи; збір доказів кібератаки для направлення до правоохоронних органів; оновлення програмного забезпечення та зміна системи паролів).

На думку авторів, саме ефективне застосування профілактичних та запобіжних заходів здатне мінімізувати вплив кіберзагроз на торгівельне мореплавство, забезпечити стабільність морських перевезень, захистити критичну інфраструктуру та підтримати довіру до галузі як до ключового елементу світової економіки.

Ключові слова: кіберзагроза, кібербезпека, кіберзлочинець, морське судно, торгівельне мореплавство, міжнародно-правові акти.

Постановка проблеми. Сучасний світ тісно пов'язаний з інформаційними технологіями, які проникають у всі сфери життя, в тому числі й у морську галузь. Однак, разом із перевагами цифрової трансформації, зростає і кількість кіберзагроз, які становлять серйозну загрозу для безпеки суден, портів та логістичних процесів. Незважаючи на зростання кіберзагроз, часто недооцінюється їхній вплив на морську галузь, що робить її вразливою до різноманітних кібератак. Зростання кіберзагроз у морській галузі є глобальною проблемою, яка вимагає негайного вирішення, оскільки потенційні наслідки таких атак можуть бути катастрофічними для світової економіки та безпеки. Відсутність єдиного підходу до оцінки та протидії кіберзагрозам у морській галузі ускладнює ефективну боротьбу з цим явищем та мінімізацію його наслідків. Тому кримінологічне дослідження кіберзагроз та їх впливу на торгівельне мореплавство, визначення системи сучасних заходів їх профілактики та запобігання є важливим та актуальним питанням у світлі необхідності формування ефективної кримінологічної політики світових держав щодо боротьби із такими негативними явищами.

Аналіз останніх досліджень і публікацій показує, що дослідження кіберзагроз привертало увагу різних вчених і зустрічалося у працях І. В. Арістова, О. М. Бандурки, А. О. Волошина, О. В. Гайдука, І. В. Діордіци, Є. О. Живило, В. В. Куцаєва, В. А. Ліпкана, О. М. Мельника, Д. С. Мініна, І. В. Сопілко, О. О. Тихомирова, В. П. Шеломенцева, В. С. Цимбалюка та інших. В той же час кримінологічні аспекти зазначеної тематики залишились малодослідженими і потребують ґрунтовного аналізу. Тому, спираючись на попередні дослідження, згідно **із метою цієї статті** авторами буде проведено всебічний кримінологічний аналіз кіберзагроз, що впливають на торгівельне мореплавство, визначено їх особливості та наслідки, розглянуто можливі заходи запобігання й профілактики з акцентуванням уваги на правових аспектах цієї тематики.

Відповідно до цього, завданнями дослідження стали: 1) кримінологічний аналіз кіберзагроз, що впливають на торгівельне мореплавство; 2) формування ключових понять у правовому врегулюванні кіберзагроз у торгівельному мореплавстві; 3) вивчення мотивів та типології кіберзлочинців у цій сфері; 4) розгляд заходів запобігання та профілактики щодо зазначених кіберзагроз.

Виклад основного матеріалу. Поняття «кіберзагроза» в сучасному світі, особливо в контексті бурхливого розвитку інформаційних технологій, набуває все більшої ваги. Воно є мінливим за характеристикою, що постійно змінює своє тлумачення під впливом нових технологій і їх впровадження у життя суспільства і зокрема у сферу торгівельного мореплавства.

Якщо спробувати визначити кіберзагрозу, то це, по суті, будь-яка загроза, що виникає в цифровому просторі і здатна завдати шкоди інформаційним системам, даним або мережам. Це може бути як цілеспрямована атака хакера, так і випадкова помилка користувача. Однак, кіберзагроза – це не просто технічний термін, а складне соціально-технічне явище, що має глибокі корені в суспільних процесах.

З точки зору свого законодавчого визначення поняття «кіберзагроза» міститься у статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» і характеризується як «наявні та потенційно можливі явища і чинники, що загрожують кібербезпеці» [1]. Із цього визначення ми бачимо, що поняття «кіберзагроза» тісно пов'язане із поняттям «кібербезпека», яка у цьому ж Законі визначається як «стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі». Також термін «кіберзагроза» активно використовується у «Стратегії кібербезпеки України», що затверджена Указом Президента України від 26 серпня 2021 року № 447/2021, де воно також переплітається із поняттями «кібербезпека» та «кіберзахист», однак не має власного тлумачення. За текстом Стратегії можна побачити, що кіберзагроза має такі властивості: технічний рівень та інструментарій реалізації; пов'язана із використанням кіберзасобів; поширюється на всі сфери життєдіяльності суспільства; може бути реальною та потенційною; несе за собою потенційно небезпечні наслідки [2].

У науці зустрічаються більш розширені визначення цього поняття. За одним підходом «кіберзагрози» описуються як протиправні та карані дії суб'єктів інформаційних правовідносин, що створюють небезпеку життєво важливим інтересам людини, суспільства та держави, а також суспільним відносинам щодо одержання, створення, зберігання, збирання, поширення, використання, охорони й захисту інформації. За іншим підходом кіберзагрози характеризуються як певні потенційно можливі явища та чинники, що створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства й держави й реалізація (наявність) яких залежить від неналежного чи недосконалого функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [4, с. 100].

З урахуванням викладеного, на думку авторів, варто акцентувати увагу саме на «потенційності виникнення» негативних явищ або процесів у кібернетичній сфері і сформулювати визначення «кіберзагрози» як сукупність негативних чинників, факторів або явищ, що за напрямком свого впливу спрямовані на пошкодження інформаційних, телекомунікаційних та інших систем, які забезпечу-

ють належне функціонування діяльності підприємств, установ, організацій або держави та захист інформації у таких системах.

Складові елементи кіберзагроз різноманітні і взаємопов'язані. Це і технічні аспекти, такі як вразливості програмного забезпечення, і людський фактор, пов'язаний з помилками користувачів, і соціальна інженерія, що використовується зловмисниками для маніпуляції людьми, які погано розбираються у інформаційних технологіях. Варто розуміти, що розвиток кіберзагроз як різновиду інформаційних загроз одночасно відбувається на двох рівнях: 1) вертикальному (за рахунок формування єдиного глобального інформаційного простору та інфраструктури у світі); 2) горизонтальному (за рахунок розвитку інформаційного суспільства як показника ефективного розвитку держави) [5, с. 129].

На сьогоднішньому етапі кіберзагрози досить сильно поширені у сфері торгівельного мореплавства, оскільки: по-перше ця сфера є вельми прибутковою за своїм економічним потенціалом, та, по-друге, тісно переплетена з цифровими технологіями. Сучасні судна – це фактично плаваючі комп'ютерні системи, де автоматизовані процеси керують рухом, навігацією, енергопостачанням тощо, забезпечують зберігання та захист даних.

Кіберзагрози у морській галузі стосуються всіх аспектів судноплавства: від управління суднами до портової інфраструктури та логістичних систем. По-перше, це, звичайно ж, технічні аспекти. Зловмисники можуть отримати несанкціонований доступ до систем керування суднами, змінити програмне налаштування навігаційного обладнання, паралізувати роботу двигунів або систем зв'язку. Зловмисники можуть проникнути в ці системи різними шляхами: через вразливості в програмному забезпеченні, через небезпечні посилання в електронних листах, що надсилаються технічному персоналу цієї системи або навіть через фізичний доступ до такого обладнання чи комп'ютерів, які здійснюють управління ним. Отримавши контроль над системою, кіберзлочинець може змінити курс судна, вимкнути двигуни, спричинити аварію судна або викрасти конфіденційні дані. Наслідки таких атак можуть бути катастрофічними, як для екіпажу судна, так і для оточуючого довкілля.

По-друге, важливу роль відіграє людський фактор, який завжди був і залишається одним із найслабших ланок у системі кібербезпеки. Кіберзлочинці часто використовують соціальну інженерію, щоб обдурити моряків та отримати доступ до їхніх облікових записів. Це можуть бути фішингові електронні листи, які маскуються під повідомлення від надійних джерел, або дзвінки від шахраїв, які видають себе за представників IT-служби компанії. Отримавши доступ до облікового запису, зловмисник може отримати контроль над системою або викрасти конфіденційну інформацію. Тому важливо проводити регулярні навчання для моряків, особливо тих, що задіяні у процесі управління торгівельним судном, щоб підвищити їхню обізнаність про кіберзагрози та навчити їх розпізнавати спроби подібного шахрайства, яке може мати загрози для самого мореплавства. Варто розуміти, що поступово все більша частина людства долучається до реалізації програм становлення безпечного інформаційного суспільства, концепцій переходу до інформаційної доби, що передбачає активне інформаційне самонавчання [7, с. 118].

По-третє, не варто забувати про те, що кібератаки на морські судна часто мають політичний підтекст. Вони можуть бути використані як інструмент гібридної війни для дестабілізації економіки супротивника, підриву довіри до його державних інституцій у питанні здатності забезпечити вільне торгівельне мореплавство або просто виступати демонстрацією власних сил та можливостей у порівнянні із конкуруючою країною. Наприклад, кібератаки можуть бути спрямовані на критичну інфраструктуру портів, що призведе до перебоїв у постачанні товарів та економічних втрат для мореплавства. Крім того, кібератаки можуть використовуватися для здійснення диверсій, таких як виведення з ладу систем навігації або керування суднами, в тому числі і військового призначення. Це може призвести до аварій, забруднення довкілля та загибелі людей унаслідок форс-мажорних обставин затоплення чи знищення судна.

Таким чином, кіберзагрози мають важливе значення у сфері торгівельного мореплавства й на міжнародному рівні держави намагаються мінімізувати їх прояви. Це можна побачити у актах міжнародно-правового врегулювання безпеки судноплавства, якими виступають, наприклад, «Міжнародний кодекс з охорони суден і портових засобів» (ISPS Code), що є додатком до «Конвенції про захист людського життя на морі» й встановлює ряд обов'язкових загальних вимог, пов'язаних із безпекою на морі та у портах, яких повинні безумовно дотримуватися уряди країн-учасниць цієї конвенції SOLAS, а також представники портової влади та судноплавних компаній. Це і «Керівництво з управління морськими кіберризиками», ухвалене Комітетом з безпеки на морі Міжнародної морської організації (IMO) у 2022 році, де описані кібернетичні загрози щодо критично вразливих елементів управління морським судном, таких як: систем управління ходовим містком; систем обробки та управління вантажем; систем управління загальним рухом судна та силовою установкою; систем контролю доступу екіпажу та пасажирів на судно тощо [5, с. 170]. Всі міжнародно-правові акти, в тому числі і «Керівництво (Рекомендації) з кібербезпеки на борту суден» 2021 року мають на меті реалізувати стратегію запобігання кіберзагрозам для забезпечення кібербезпеки та належного розвитку торгівельного мореплавства.

При цьому варто не забувати про кримінологічні аспекти кіберзагроз, вивчення яких має не менше значення, ніж дослідження міжнародно-правових стандартів. Адже кримінологічні аспекти визначають мотивацію та типологію кіберзлочинця, що створює такі потенційні кіберзагрози для різних сфер економічної діяльності, в тому числі і для торгівельного мореплавства.

Щоб ефективно протистояти кіберзагрозам у морській галузі, необхідно глибоко розуміти мотивацію та поведінку кіберзлочинців. Адже саме розуміння детермінант (причин), які спонукають людей до здійснення кіберзлочинів, дозволяє розробити ефективні заходи профілактики та протидії.

Детермінанти та мотивація кіберзлочинця в більшості випадків включає в себе бажання отримати фінансову вигоду, оскільки отримання значних фінансових ресурсів від кібератаки є першочерговим мотивуючим стимулом для її здійснення. Кіберзлочинці можуть отримувати незаконний прибуток шляхом викрадення конфіденційної інформації про морську компанію, про напрямки руху й вантаж її суден, про взаємовідносини з контрагентами, про наявність критично важливих поставок або іншу комерційну інформацію, що матиме цінність

і попит у конкурентів компанії. У подальшому викуп може бути пов'язаний або з нерозголошенням отриманої інформації або ж з продажом такої інформації зацікавленим особам (конкурентам). З точки зору технічної атаки на програмні процеси можливе блокування автоматизованих систем судна з метою зупинення роботи компанії на невизначений час, зміни курсу судна, вимагання викупу за відновлення роботи мереж тощо.

На другому місці у мотивації стоїть питання усунення конкурентів компанії задля чого конкуруючою компанією може бути умисно найнята організована група кіберзлочинців, яка спеціалізується на кібератаках, пов'язаних із тривалим виведенням з ладу автоматизованих систем судна чи портової інфраструктури. У випадку успішності такої атаки компанія отримує можливість просунутися на ринку за рахунок тимчасового виведення конкуренту із бізнесу. Такі кіберзагрози постійно переслідують успішні компанії у сфері торгівельного мореплавства, що вимагає від них посиленого захисту власних автоматизованих процесів та постійного моніторингу активності конкурентів на ринку.

На третьому місці знаходяться особисті мотиви помсти та ідеологічні мотиви, коли мова йде про колишніх працівників компанії, які з певних причин втратили або вимушені були залишити роботу. Такі особи, маючи конфіденційну інформацію про певні аспекти роботи компанії або її суден, отриману у процесі їх трудової діяльності, є потенційною «знахідкою» для кіберзлочинців у питанні пошуку «слабких місць» у роботі компанії, що впливає на рівень кіберзагроз. Крім того, можуть зустрічатися й ідеологічно мотивовані особи, які прагнуть дестабілізувати роботу портів як критичної інфраструктури у морській сфері або просто завдати шкоди певним країнам чи компаніям у зв'язку з впливом певної ідеології. У сукупності особиста або ідеологічна спрямованість складає незначний відсоток кіберзагроз, оскільки вона не може бути реалізована без зв'язків із професійними кіберзлочинцями, однак при цьому вона складніше піддається оцінці.

Таким чином, перелічене визначає типологію кіберзлочинців у сфері торгівельного мореплавства, яка базується на комерційному напрямку і необхідності мати значний професійний досвід. Зазвичай повноцінно працюють саме організовані хакерські групи, які прямо спеціалізуються на роботі із автоматизованим програмним забезпеченням судна або порту. При цьому серед них є розповсюдженими державні спонсоровані хакери, що представляють собою кіберзлочинців, які діють за завданням урядів своїх країн. Їхні цілі можуть бути різноманітними: від економічного шпіонажу до дестабілізації певної країни-супротивника. Рідше у цій сфері зустрічаються одиночні хакери, які повинні мати значні ресурси і досвід. В переважній більшості випадків всі дії кіберзлочинців виконуються у межах певного найму, за замовленням інших осіб або організацій.

Із викладеного можна побачити, що протидія кіберзагрозам у сфері торгівельного мореплавства вимагає комплексного підходу, який охоплює різні аспекти діяльності торгівельної компанії або порту. Для ефективної боротьби із кіберзагрозами варто використовувати не лише запобіжні, але й профілактичні заходи, оскільки саме застосування профілактичних заходів допомагає значно зменшити рівень кіберзагроз і мінімізувати їх наслідки.

Перш за все, ключовим елементом профілактики є підвищення обізнаності та кіберкультури серед персоналу морських компаній, портових служб та інших

учасників галузі. Навіть найсучасніші технології захисту будуть неефективними, якщо працівники не усвідомлюють ризиків та не знають, як діяти у разі кібератаки. Тому регулярне навчання, тренінги та симуляції кібератак мають стати обов'язковою частиною підготовки кадрів. Це дозволить мінімізувати людський фактор, який часто стає слабкою ланкою у системі кібербезпеки.

Другим важливим напрямом є розробка та впровадження сучасних технічних засобів захисту, зокрема криптозахист паролів [3, с. 230]. Суднові системи, портова інфраструктура та логістичні мережі повинні бути оснащені надійними паролями, мережевими екранами, системами виявлення вторгнень, антивірусними програмами та іншими інструментами кіберзахисту. Особливу увагу слід приділити захисту критично важливих систем, таких як системи навігації, управління двигунами та зв'язку, оскільки їх компрометація може призвести до катастрофічних наслідків. Крім того, важливо забезпечити регулярне оновлення програмного забезпечення та проведення аудитів безпеки для виявлення потенційних вразливостей.

Третім елементом стратегії профілактики є розробка та дотримання міжнародних стандартів і нормативних актів у сфері кібербезпеки. На сьогодні існують міжнародні ініціативи, такі як рекомендації Міжнародної морської організації (ІМО) щодо кібербезпеки, які покликані забезпечити єдиний підхід до захисту морської інфраструктури. Дотримання цих стандартів, а також розробка національних законодавчих актів, що регулюють кібербезпеку в мореплавстві, дозволять створити правову основу для боротьби з кіберзагрозами.

Четвертим важливим аспектом є створення системи оперативного реагування на кіберзагрози та кіберінциденти. У разі кібератаки швидкість та координація дій мають вирішальне значення. Тому морські компанії та портові оператори повинні мати чіткі плани дій на випадок кіберінцидентів, включаючи механізми відновлення систем, взаємодію з правоохоронними органами та міжнародними організаціями. Створення спеціалізованих центрів реагування на кіберзагрози в мореплавстві може значно підвищити ефективність боротьби з такими інцидентами.

Нарешті, важливим напрямом профілактики є міжнародна співпраця та обмін інформацією. Кіберзагрози не мають кордонів, тому ефективна боротьба з ними можлива лише за умови координації зусиль на міжнародному рівні. Обмін даними про нові загрози, методи атак та найкращі практики захисту дозволить краще підготуватися до потенційних викликів. У цьому контексті важливу роль відіграють міжнародні організації, такі як ІМО, Інтерпол та інші, які можуть виступати платформами для такого співробітництва.

У разі, коли кіберзагроза переростає у реальну кібератаку, ефективність дій із її припинення (запобігання) та мінімізації наслідків залежить від наявності чіткого плану реагування, координації між усіма учасниками процесу та швидкості впровадження заходів. Першим кроком у такій ситуації є ідентифікація та аналіз загрози. Необхідно оперативно визначити джерело атаки, її характер (наприклад, DDoS-атака, шкідливе програмне забезпечення, фішинг тощо) та масштаби впливу на системи. Для цього використовуються спеціалізовані інструменти моніторингу та аналізу мережевої активності, які дозволяють виявити аномалії та потенційні загрози.

Після ідентифікації загрози необхідно ізолювати уражені системи для запобігання поширення атаки. Наприклад, якщо атака спрямована на суднову систему навігації, її слід відключити від загальної мережі, щоб уникнути компрометації інших пристроїв. У портовій інфраструктурі це може включати тимчасове відключення певних серверів або мережевих сегментів. Ізоляція дозволяє локалізувати загрозу та запобігти її ескалації. Важливим елементом є комунікація з усіма зацікавленими суб'єктами, які задіяні у діяльності компанії задля уникнення паніки. У разі кібератаки на морську інфраструктуру необхідно інформувати екіпаж судна, портові служби, клієнтів та партнерів про ситуацію та вжиті заходи. Це дозволяє уникнути паніки, забезпечити прозорість та підтримати довіру до компанії.

Наступним кроком є активне протидіяння атаці. Це може включати використання антивірусних програм для блокування шкідливого програмного забезпечення, налаштування мережевих екранів для блокування підозрілих IP-адрес або застосування інших технічних засобів для нейтралізації атаки. У випадках, коли атака має складний характер, може знадобитися залучення кібербезпекових експертів або спеціалізованих організацій, які зможуть провести глибокий аналіз та розробити стратегію протидії.

Одночасно з технічними заходами важливо забезпечити правове реагування. Це включає збір доказів атаки (наприклад, лог-файлів, даних про мережеву активність тощо) для направлення до правоохоронних органів, подальшого розслідування та притягнення винних до відповідальності. У багатьох країнах існують спеціалізовані підрозділи правоохоронних органів, які займаються кіберзлочинністю, тому важливо оперативно повідомити про інцидент та надати всю необхідну інформацію. Після припинення атаки необхідно провести відновлення систем та їхню повторну перевірку. Це включає оновлення програмного забезпечення, зміну паролів, впровадження додаткових заходів безпеки та проведення аудиту для виявлення потенційних вразливостей. Також важливо провести аналіз інциденту, щоб виявити причини успіху атаки та розробити заходи для запобігання подібним ситуаціям у майбутньому.

Висновки і пропозиції. Узагальнюючи проведене дослідження, можна дійти висновків, що кіберзагрози становлять значний обсяг ризиків у діяльності морських компаній та морської інфраструктури у сфері торгівельного мореплавства. Авторами було розглянуто поняття кіберзагрози у контексті неналежного чи недосконалого функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, досліджено складові елементи кіберзагрози у сфері торгівельного мореплавства, посилання на які є у актах міжнародно-правового врегулювання безпеки судноплавства. За рахунок дослідження кримінологічних аспектів кіберзагроз та мотивації кіберзлочинця авторами було сформовано систему постійних профілактичних та запобіжних заходів, що мають реалізовуватися суб'єктами, задіяними у сфері торгівельного мореплавства. Саме ефективне застосування профілактичних та запобіжних заходів здатне мінімізувати вплив кіберзагроз на торгівельне мореплавство, забезпечити стабільність морських перевезень, захистити критичну інфраструктуру та підтримати довіру до галузі як до ключового елементу світової економіки.

Список використаної літератури

1. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 05.10.2017 року. Відомості Верховної Ради України. 2017. № 45. Стор. 42. Ст. 403.
2. Стратегія кібербезпеки України: затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. Офіційний вісник України. 2021. № 70. Стор. 42. Ст. 4417.
3. Гайдук О. В., Звєрєв В. П. Аналіз кіберзагроз в умовах стрімкого розвитку інформаційних технологій. Кібербезпека: освіта, наука і техніка. 2024. № 3. С. 225-236.
4. Діордіца І. В. Поняття і зміст кіберзагроз на сучасному етапі. Підприємництво, господарство і право. 2017. № 4. С. 99-106.
5. Ліпкан В. А. Правові засади розвитку інформаційного суспільства в Україні : [монографія] / В. А. Ліпкан, І. М. Сопілко, В. О. Кір'ян / за заг. ред. В. А. Ліпкана. Київ: ФОП О. С. Ліпкан, 2015. 664 с.
6. Мельник О. М., Волошин А. О., Пуляєв І. О., Бурлаченко Д. А., Щенявський Г. С. Огляд міжнародної практики забезпечення кібербезпеки в морській галузі. Міжнародний науковий журнал «Інтернаука». 2022. № 10. С. 167-171.
7. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави : монографія / О. О. Тихомиров; заг. ред. Р. А. Калюжний. Центр навчально-наукового та науково-практичного видання НА СБ України, 2014. 196 с.

References

1. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 № 2163-VIII. Vidomosti Verkhovnoi Rady Ukrainy. 2017. № 45. Stor. 42. St. 403 [in Ukrainian].
2. Stratehiya kiberbezpeky Ukrainy: zatverdzhena Ukazom Prezydenta Ukrainy vid 26.08.2021 № 447/2021. Ofitsiinyi visnyk Ukrainy. 2021. № 70. Stor. 42. St. 4417 [in Ukrainian].
3. Haiduk O. V., Zvieriev V. P. (2024). Analiz kiberzahroz v umovakh strimkoho rozvytku informatsiinykh tekhnolohii. Kiberbezpeka: osvita, nauka i tekhnika, 3, 225-236 [in Ukrainian].
4. Diordytsa I. V. (2017). Poniattia i zmist kiberzahroz na suchasnomu etapi. Pidpryiemnytstvo, hospodarstvo i pravo, 4, 99-106 [in Ukrainian].
5. Lipkan V. A. (2015) Pravovi zasady rozvytku informatsiinoho suspilstva v Ukraini: monohrafiia / V. A. Lipkan, I. M. Sopilko, V. O. Kirian; za zah. red. V. A. Lipkana. Kyiv: FOP O. S. Lipkan, 664 [in Ukrainian].
6. Melnyk O. M., Voloshyn A. O., Pulaiev I. O., Burlachenko D. A., Shcheniavskyi H. S. (2022). Ohliad mizhnarodnoi praktyky zabezpechennia kiberbezpeky v morskii haluzi. Mizhnarodnyi naukovyi zhurnal «Internauka», 10, 167-171 [in Ukrainian].
7. Tykhomyrov O. O. (2014). Zabezpechennia informatsiinoi bezpeky yak funktsiia suchasnoi derzhavy: monohrafiia / O. O. Tykhomyrov; zah. red. R. A. Kaliuzhnyi. Tsentr navchalno-naukovoho ta naukovo-praktychnoho vydannia NA SB Ukrainy, 196 [in Ukrainian].

Стаття надійшла 15.02.2025 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

I. A. Osadcha, Lawyer, Senior Lecturer
Odesa National University of Technology
the Department of Philosophy and Law
112 Kanatna St, Odesa, 65039, Ukraine
e-mail: pravnic@ukr.net
ORCID iD: https://orcid.org/0000-0002-9243-1064

CRIMINOLOGICAL ANALYSIS OF CYBER THREATS AND THEIR IMPACT ON COMMERCIAL SHIPPING

Summary

The article is devoted to a criminological study of cyber threats and their impact on cybersecurity in the field of commercial shipping, which is an important and relevant issue for the development of a system of measures for their prevention and mitigation. A cyber threat is a set of negative factors, elements, or phenomena aimed at damaging information, telecommunications, and other systems that ensure the proper functioning of enterprises, institutions, organizations, or the state, as well as the protection of information within such systems. Cyber threats target cybersecurity, which encompasses the state of complete protection of the vital interests of individuals, society, and the state in cyberspace.

The authors identifies the components of cyber threats in the field of commercial shipping, which include technical aspects of the operation of automated ship and port infrastructure systems, software vulnerabilities, the human factor, and social engineering related to errors made by users with limited knowledge of information technology. The international legal regulation of cyber threats is analyzed, covering the International Ship and Port Facility Security Code (ISPS Code), the Guidelines on Maritime Cyber Risk Management (adopted by the Maritime Safety Committee of the International Maritime Organization, IMO), the Guidelines on Cybersecurity Onboard Ships, and others.

At present, cyber threats are widespread in the field of commercial shipping because, firstly, this sector is highly profitable in terms of economic potential, and secondly, it is closely intertwined with digital technologies. Modern ships are essentially floating computer systems where automated processes control movement, navigation, power supply, and more, while also ensuring data storage and protection.

The authors examines the determinants and motivations of cybercriminals in this field (financial gain, elimination of competitors, motives of revenge, ideological motives) and formulates key measures for the prevention and mitigation of cyber threats in commercial shipping, which include:

- raising awareness and cybersecurity culture among personnel of maritime companies, port services, and other industry participants;

- developing and implementing modern technical protection tools (intrusion detection systems, password encryption, firewalls) in ship systems, port infrastructure, and logistics networks;

- developing and adhering to international standards and regulatory acts of the IMO in the field of cybersecurity, as well as fostering international cooperation and information exchange;

- establishing a system for rapid response to cyber threats and cyber incidents (identification and analysis of threats; isolation of affected systems to prevent the spread of attacks; blocking malicious software and restoring system functionality; collecting evidence of cyberattacks for submission to law enforcement agencies; updating software and changing password systems).

In the authors opinion, the effective application of preventive and mitigation measures can minimize the impact of cyber threats on commercial shipping, ensure the stability of maritime transportation, protect critical infrastructure, and maintain trust in the industry as a key element of the global economy.

Keywords: cyber threat, cybersecurity, cybercriminal, maritime vessel, commercial shipping, international legal acts.