УДК 356.2:346.7; 336.7:340.5; 346.764,477
DOI https://doi.org/10.32782/pdu.2024.2.4

Е. П. Іванченко
кандидат юридичних наук, професор
Української технологічної академії,
докторант
Науково-дослідного інституту приватного права
і підприємництва імені академіка Ф. Г. Бурчака
Національної академії правових наук України,
радник Асоціації митних брокерів України

АКТУАЛЬНІ ПИТАННЯ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА КІБЕРСТРАХУВАННЯ МИТНОГО ПРОСТОРУ УКРАЇНИ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ УДОСКОНАЛЕННЯ

Стаття присвячена дослідженню правового забезпечення кібербезпеки митного простору України в сучасних економіко-правових умовах за напрямами основних засад державної митної політики у цій сфері та кіберстрахування як ефективного фінансового механізму захисту прав та законних інтересів учасників митних правовідносин від фінансових збитків, що можуть бути спричинені митними кіберінцидентами.

Аналіз правової доктрини з досліджуваних питань і митного законодавства України, дозволив автору сформулювати висновок відносно того, що процеси тотальної діджиталізації митного простору України актуалізують потребу кіберзахисту, з метою забезпечення сталості митного кіберпростору, як віртуального простору, що надає можливості здійсненню реалізації митних відносин, який утворений внаслідок функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням Інтернет та (або) інших глобальних мереж передачі даних.

Глобальна цифровізація зумовлює кардинальні трансформаційні зміни митної сфери, роблячи її вразливою до нових типів кіберзагроз. Паралельно спостерігається посилення митної кібербезпеки більшості країн світу.

Діджиталізація митного простору України актуалізує ризики посилення кібератак. Автор відзначає, що серед основних чинників, що сприяють цьому, можна виділити наступні: невідповідність митної інфраструктури сучасним вимогам кібербезпеки, недостатній рівень захищеності митної інформаційної інфраструктури та державних електронних ресурсів, відсутність системного підходу до кіберзахисту та дієвих інструментів убезпечення кіберризиків, недосконалість організаційно-технічної інфраструктури забезпечення кібербезпеки, а також недостатня ефективність митних органів у протидії кіберзагрозам та слабка координація між суб'єктами митної кібербезпеки.

Автор доводить, що ключовим аспектом розвитку безпечного митного кіберпростору є проактивна державна політика в галузі митної кібербезпеки. Ця політика повинна забезпечувати постійну адаптацію до мінливого кіберсередовища та сприяти інтеграції національних систем митної кібербезпеки у глобальний контекст, дотримуючись найвищих міжнародних стандартів.

За результатами дослідження, автор формулює висновок про те, що митні кіберризики характеризуються складною природою і потребують фінансового убезпечення – кіберстрахування, а процес такого убезпечення – належного нормативного унормування.

Ключові слова: *митна реформа України, державна митна політика, митна справа, електронна митниця, цифрова трансформація митного простору, митний кіберпростір, кібербезпека митного простору, митний кіберризик (кіберзагроза), кіберстрахування митних ризиків.*

Постановка проблеми. Активне упровадження цифрових технологій у митний простір України та діджитал-модернізація митної справи має стати пріоритетом державної митної політики та ключовим елементом стратегії повоєнного економічного відновлення України.

Згідно сучасних світових практик, пришвидшення та підвищення якості митних процедур забезпечується шляхом спрощення і автоматизації існуючих процесів та зменшення впливу людського фактора. При цьому, в контексті набуття Україною статусу кандидата у члени ЄС, інформаційно-телекомунікаційні системи (ІКС) митниці мають бути сумісними з аналогічними системами інших країн, передусім із ЄС, що потребує зменшення відмінностей у митних процедурах, забезпечення миттєвого обміну інформацією та вимагає забезпечення високого рівня безпеки електронних ресурсів.

Наведене дозволяє стверджувати про активне формування економіко-правового феномену – *митного кіберпростору України*. Така формація потребує правового та організаційного упровадження основних засад захисту митних інтересів і митної кібербезпеки України та визначення пріоритетних напрямів державної митної політики у цій сфері.

Вважаємо, що цифрова трансформація митного простору та осучаснення митних процедур є важливими складовими виконання міжнародних зобов'язань України, згідно Угоди про асоціацію між Україною та Європейським Союзом (Угода про асоціацію) [1] і вимагають нагального нормативно-правового врегулювання питань забезпечення кібербезпеки митного простору України.

Належне нормативне забезпечення безпеки митного кіберпростору України на етапі формування спеціального законодавства має відбуватися паралельно за двома пріоритетними векторами, де:

за першим – необхідно визначити і унормувати основний категоріально-термінологічний апарат (митна кіберзагроза (митний кіберризик), митний кіберінцидент, митна кібератака тощо), порядок, вимоги та заходи із забезпечення кіберзахисту митного кіберпростору, основні цілі, напрями та принципи державної політики у цій сфері, повноваження державних органів та основні засади координації їхньої діяльності із забезпечення митної кібербезпеки;

за другим – необхідно визначити і нормативно врегулювати основні інструменти фінансового убезпечення митного кіберпростору України від потенційних кіберризиків, що можуть завдати збитків (шкоди) учасникам митних правовідносин.

На нашу думку, у контексті постійного зростання кіберзагроз, саме інструмент кіберстрахування набуває статусу ефективного та оперативного фінансового механізму захисту прав та законних інтересів учасників митних правовідносин від фінансових збитків, що можуть бути спричинені митними кіберінцидентами.

Аналіз останніх досліджень і публікацій. Протягом останніх років спостерігається значний науковий інтерес до аналізу різноманітних аспектів кібербезпеки та кіберстрахування. Дослідженнями в цій галузі знань займаються як юристи, так і економісти та фахівці з кібербезпеки.

Теоретичним фундаментом дослідження в сфері правового регулювання кібербезпеки та кіберзахисту слугують розробки вітчизняних і зарубіжних фахівців. Означену проблематику досліджували такі вчені, як: Н. Ткачук, Ю. Даник, П. Воробієнко, В. Чернега, Г. Андрощук, Т. Кваша, А. Махнюк, О. Кириченко, А. Войцехівський, В. Хаустова, О. Решетняк, М. Хаустов, В. Зінченко та інші. В частині вивчення питань правового регулювання відносин із кіберстрахування дослідження провадили: В. Братюк, У. Тихонько, С. Перцева, Н. Пацурія, О. Заярний, Г. Мамонова, Л. Позднякова, Л. Гуменюк та інші.

Проте, комплексному дослідженню питань правового забезпечення кібербезпеки та кіберстрахування митного простору України у науковому юридичному полі до цього часу не приділялася належна увага, що зумовлює актуальність цієї тематики.

Мета статті. Метою статті є дослідження правового забезпечення кібербезпеки митного простору України в сучасних економіко-правових умовах за напрямами

основних засад державної митної політики, що на сьогодні склалися, та кіберстрахування як ефективного фінансового механізму захисту прав та законних інтересів учасників митних правовідносин від фінансових збитків, що можуть бути спричинені митними кіберінцидентами.

Виклад основного матеріалу. Ідея цифрової трансформації єдиної митної території України не є новою.

Варто відзначити, що упровадження митних інформаційно-комунікаційних технологій (ІКТ) в Україні розпочалося ще у 1992 році, а імплементація системи «Електронна митниця» була практично впроваджена з 2005 року. У 2006 році було започатковано необхідні умови для використання цифрових та ІКТ електронного документообігу з допомогою електронного цифрового підпису, який на основі відповідного програмного забезпечення дав змогу оптимізувати процеси електронного декларування між митними органами держави та суб'єктами ЗЕД [2, 321].

17 вересня 2008 року Розпорядженням Кабінету Міністрів України № 1236-року була схвалена «Концепція створення багатофункціональної комплексної системи «Електронна митниця»» з окресленням трьох етапів її реалізації (до кінця 2025 року) [3]. Важливим кроком на етапі запровадження багатофункціональної комплексної системи «Електронна митниця» стало прийняття Концепції інтегрування системоутворюючих компонентів технічних та спеціальних засобів митного контролю з автоматизованою системою митного оформлення Державною митною службою України (Держмитслужба) [2, 321].

Основою нормативного регулювання процесів діджитал-оновлення митного простору України є положення Митного Кодексу України (МК України) [4], згідно зі ст. 31 якого, митна справа здійснюється з використанням ІКТ, у тому числі заснованих на системах, що забезпечують функціонування електронних інформаційних ресурсів митних органів, і засобів їх забезпечення, що функціонують на національному та (або) міжнародному рівні.

Оскільки Україна наближається до набуття повноправного членства в ЄС, то головним і актуальним залишається завдання вдосконалення діяльності митних органів у напрямку діджиталізації процесів, шляхом спрямування зусиль на спрощення та створення сприятливих умов для суб'єктів зовнішньоекономічної діяльності (ЗЕД) [5].

Міжнародний рівень забезпечення використання ІКТ у митній справі полягає, перш за все, у виконанні зобов'язань прийнятих на себе Україною за Угодою про асоціацію. Згідно Додатку XV до Глави 5 якої, адаптація національного законодавства до права ЄС за напрямом «митне законодавство» – є пріоритетом державної митної політики.

Щодо конструктивності дій на шляху України до діджиталізації основних процесів у митному просторі свідчить Висновок Єврокомісії стосовно заявки на членство в ЄС [6], який було оприлюднено у лютому 2023 року і в якому відзначено, що оцінка виконання розділу «Наближення митного законодавства» становить – 4-й із 5 можливих рівнів.

При цьому, Єврокомісія наголосила на подальших необхідних напрямах розвитку митної справи задля досягнення євроінтеграційного прогресу, зокрема вказала на обов'язковість: доопрацювання ІТ-системи для надання авторизацій; розвиток та вдосконалення митних ІТ-систем; удосконалення поточних процедур та методів роботи у деяких операційних сферах для покращення імплементації та дотримання митного законодавства, адаптованого до вимог ЄС тощо.

Попри триваючу повномасштабну військову агресію із боку РФ проти України, та введення правового режиму воєнного стану, наша держава продовжує активно упроваджувати та законодавчо унормовувати процедури діджиталізації митного простору України. Протягом 2022–2024 років прийнято низку нормативно-правових актів, що врегульовують окремі аспекти діджиталізації митної справи. Основними напрямами правового забезпечення упровадження діджитал-технологій в митному просторі України є: 1) процедура спільного транзиту;

2) технологічні інструменти: «Єдине вікно для міжнародної торгівлі», «єЧерга», «Електронна митниця»; 3) діджиталізація процедури ввезення гуманітарної допомоги; 4) окремі аспекти діджиталізації митної брокерської діяльності; 5) діджиталізація митної справи тощо.

Упровадження діджитал-інструментарію у митну справу надає змоги суттєво змінити ставлення суб'єктів ЗЕД та митних брокерів до митної системи України, створити сприятливі та спрощені умови здійснення експортно-імпортних операцій та посилити захист економічної безпеки держави, як в період дії правового режиму воєнного стану, так і у період повоєнного економічного відновлення України.

Вищенаведеними окремими прикладами врегулювання різних напрямів діджиталізації митного простору України, доводиться факт практичної реалізації виконання Україною зобов'язань, прийнятих на себе згідно Угоди про асоціацію в сфері цифрової трансформації митної справи, що нами раніше неодноразово досліджувалося [7; 8; 9].

Варто відзначити, що цифровізація кардинально позначилася на суспільних відносинах, додавши не лише позитивні моменти (широкі можливості для розвитку відповідних сфер та функціонування суспільства в умовах сучасних загроз суспільному благополуччю, серед яких коронавірусна пандемія та російська агресія проти України), але й привнісши додаткові ризики, пов'язані зі зловживанням цифровими можливостями [10].

Процеси тотальної діджиталізації митного простору України актуалізують потребу кіберзахисту з метою забезпечення сталості *митного кіберпростору*, як віртуального простору, що надає можливості здійсненню реалізації митних відносин, який утворений внаслідок функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням Інтернет та (або) інших глобальних мереж передачі даних.

Для України питання забезпечення безпеки у кіберпросторі та мінімізації потенційних і реальних кіберзагроз та кіберризиків гостро постало з 2014 року, коли РФ здійснила вторгнення на територію України та незаконно анексувала частину суверенної території і активізувалося у 2022 році, з моменту повномасштабної військової агресії. Перехід глобальних соціополітичних комунікацій у «цифру», аспектує прояв негативних наслідків різного виду загроз та ризиків, основними із яких є кіберзагрози та кіберризики, реалізація яких від'ємно впливає як на загальну систему національної безпеки, так і на економіку будь-якої країни в сучасному світі. Усі вищеозначені процеси (як зовнішні, так і внутрішні) зумовили посилення уваги законодавця до нормативного удосконалення відносин у сфері забезпечення кібербезпеки та кіберзахисту [11, с. 90].

Вважаємо за доцільне в межах цієї наукової роботи зупинитися на проблематиці правового забезпечення кібербезпеки митного простору України в сучасних економіко-правових умовах за напрямами основних засад державної митної політики та кіберстрахування як ефективного фінансового механізму захисту прав та законних інтересів учасників митних правовідносин від фінансових збитків, що можуть бути спричинені митними кіберінцидентами.

Системоутворюючими, в частині *діджиталізації митної справи як напряму державної митної політики*, слід визначити таки відомчі нормативно-правові акти як Наказ Міністерства фінансів України від 19 травня 2023 року № 263 «Про затвердження Положення про Єдину автоматизовану інформаційну систему митних органів, порядок і умови застосування її систем» (Наказ № 263) [12] і Наказ Міністерства фінансів України від 9 лютого 2024 року № 63 «Про реалізацію рішення Комітету з управління інформаційними технологіями у системі управління державними фінансами» (Наказ № 63) [13], яким було реалізовано рішення Комітету з управління інформаційними технологіями у системі управління державними фінансами (Комітет) «Про затвердження довгострокового національного стратегічного плану цифрового розвитку, цифрових трансформацій і цифровізації Державної митної служби України та її територіальних

підрозділів на основі Багаторічного стратегічного плану електронної митниці ЄС (Multi-Annual Strategic Plan For Electronic Customs, MASP-C)» (План) [14].

Згідно Наказу № 263 Єдина автоматизована інформаційна система митних органів (ЄАІС) – багатофункціональна інтегрована автоматизована система, яка становить сукупність взаємопов'язаних інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, що забезпечують функціонування електронних інформаційних ресурсів митних органів з метою здійснення митної справи, і засобів їх забезпечення.

Наказ № 63, який затвердив План, розроблений у контексті підготовки України до вступу до ЄС та виконання Додатку XV до Угоди про асоціацію, яким встановлено чіткий перелік заходів, що їх Україна має виконати задля гармонізації митних процесів з європейськими стандартами. Особливу увагу було приділено виконанню всіх вимог щодо майбутніх інтеграцій до систем ЄС.

План має стати керівним документом з питань упровадження та розвитку митних інформаційних систем у наступні роки. Успішна реалізація визначених трансформацій забезпечить ІТ-систему адекватними інструментами для боротьби з корупцією та шахрайством.

Як основу ІТ-стратегії Держмитслужби визначено, зокрема: сервісно-орієнтовну архітектуру; централізоване упровадження ЄАІС; гармонізований інтерфейс із ЄС і Єдине вікно для міжнародної торгівлі.

Особлива увага нормотворця, в напрямі врегулювання процесів діджиталізації митної справи, приділена упровадженню безпаперових процедур у митному просторі України. У митній справі для цього реалізується Ініціатива електронної митниці (Electronic customs initiative). З цією метою, у процесі ІТ-трансформації Держмитслужба використовуватиме управління бізнес-процесами та BPM-моделювання, що дозволить забезпечити цілісне уявлення про митні процеси та практичні наслідки їх упровадження відповідно до митного законодавства України та ЄС.

Аналізований План, в частині реалізації заходів, щодо побудови надійних та сучасних ІТ-систем Митниці, розрахований до 2026 року включно та передбачає залучення міжнародної технічної допомоги.

Згідно Наказу № 63, головною метою Плану є формування дорожньої карти цифрової трансформації та розвитку Держмитслужби для забезпечення якісно нових зручних, надійних та прискорених процесів митної справи в Україні, яка базується на передових міжнародних практиках та рекомендаціях. Означеної мети можна досягти шляхом побудови сучасних, гнучких, надійних, сервісно-орієнтованих інформаційно-комунікаційних систем, заміни та модернізації застарілих функціонуючих систем, зокрема Єдиної автоматизованої інформаційної системи митних органів (ЄАІС), її складової – автоматизованої системи митного оформлення (АСМО), з урахуванням передових міжнародних практик, що базуються на чинному законодавстві ЄС, положеннях Митного кодексу України, орієнтованих на спрощення та гармонізацію митних процедур, створення ефективного та прозорого торговельного середовища, покращення позиції України у світових рейтингах, пов'язаних із легкістю ведення бізнесу.

Основними напрямами упровадження цифрової трансформації та розвитку Держмитслужби на сьогодні є: спрощення митних процедур завдяки використанню стандартизованих європейських митних процесів та широкого використання інформаційних технологій; розвиток інформаційного обміну з митними органами сусідніх держав для прискорення митних формальностей та зменшення процедурних навантажень на бізнес; модернізація систем та упровадження нових рішень для створення нового сервіс-орієнтованого ландшафту інформаційно-комунікаційних систем європейського зразка; трансформація та розвиток кадрового забезпечення Держмитслужби для оновлення процесів управління ІТ; забезпечення можливостей безпечного та безперервного функціонування критичних інформаційно-комунікаційних систем Держмитслужби.

Розвиток Держмитслужби на поточний час здійснюється в умовах зовнішніх та внутрішніх викликів та загроз: збільшення обсягів транскордонної торгівлі та

торгівлі товарами через мережу Інтернет, що пересилаються в міжнародних поштових відправленнях, а також товарів, що доставляють експрес-перевізники; посилення міжнародної та внутрішньогалузевої конкуренції, що потребує підвищення конкурентоспроможності у митній сфері та скорочення термінів проведення митних операцій; поява нових способів та методів скоєння злочинів та адміністративних правопорушень у сфері зовнішньоекономічної діяльності в умовах розвитку інформаційних технологій; збільшення загроз можливого несанкціонованого доступу до ЄАІС з боку глобального інформаційного простору; відсутність сталих процесів розробки, тестування та упровадження комплексних та складних наявних інформаційно-комунікаційних систем; складність підвищення кваліфікації наявних та залучення на службу до митних органів нових висококваліфікованих кадрів у зв'язку з недостатнім рівнем економічної мотивації та відсутності необхідних механізмів.

Для реалізації основних завдань Держмитслужби та подолання наявних викликів та загроз Наказом № 63 визначені певні цільові орієнтири. Дотичними до проблематики нашого дослідження є цільові орієнтири 1 та 7. Зміст цільового орієнтиру 1 полягає у: повномасштабній цифровізації та автоматизації діяльності митних органів, які включають: цифрову трансформацію технологій митного оформлення та митного контролю до та після випуску товарів з використанням методів штучного інтелекту та обробки великих обсягів даних; застосування інтелектуальної системи управління ризиками; упровадження технологій, які забезпечують автоматичне здійснення митних операцій без участі посадових осіб у місцях переміщення товарів через митний кордон; створення довгострокових архівів юридично значущих електронних документів; застосування міжнародних електронних систем верифікації та сертифікації походження товарів; автоматизацію процесу контролю правильності класифікації товарів та виявлення порушень, пов'язаних із наданням недостовірних відомостей про класифікаційний код товарів згідно з УКТ ЗЕД; застосування інтегрованих механізмів міжвідомчої інформаційної взаємодії; участь у створенні національного механізму «єдиного вікна» шляхом розвитку та модернізації «Єдиного вікна для міжнародної торгівлі», забезпеченні поєднання із системами «єдиного вікна» митних служб країн ЄС.

Цільовий орієнтир 7 спрямований на побудову проектів захищеної інформаційної системи Держмитслужби, що передбачає упровадження: цілісної архітектури кібербезпеки в інформаційно-комунікаційній системі Держмитслужби; системи управління привілейованим доступом – Privileged Account Management (PAM); функціоналу комплексного аудиту поточних правил на мережевих екранах – Firewall Audit (FW Audit); функціоналу захисту вебдодатків від поширених атак – Web Application Firewall (WAP); функціоналу виявлення загроз та реагування на них – Extended Detection & Response (XDR); функціоналу виявлення, оцінки та усунення вразливостей – Vulnerability Management (VM); вебшлюзу інформаційної безпеки для фільтрації вебтрафіку – Web Security Gateway (WSG); функціоналу багатофакторної аутентифікації – Multi-Factor Authentication (MPA); функціоналу запобігання витоку інформації – Data Loss/Leak Prevention (DLP); програмно-керованої платформи Secure Access Service Edge (SASE) з вбудованим IP-шифруванням та сервісами доступу за принципом нульової довіри Zero-Trust Network Access (ZTNA); функціоналу контролю доступу до мережі – Network Access Control (NAC); функціоналу уніфікованого управління кінцевими точками та мобільними пристроями – Unified Endpoint Management (UEM).

Наведені напрями та орієнтири побудови глобального цифрового митного простору вимагають захисту від кіберзагроз як наявних та потенційно можливих явищ і чинників, що створюють небезпеку митним інтересам України у митному кіберпросторі, мають негативний та (або) послаблюючий вплив на стан кібербезпеки України та кіберзахист її об'єктів.

Розуміючи можливість настання означених кіберзагроз, що при їх реалізації перетворюються на конкретні кіберри-

зики і втілюються у окремих кіберінцидентах Наказом № 63 закріплені *принципи кіберзахисту*, сутність яких полягає у наступному: захищеність даних передбачає забезпечення цілісності, доступності, конфіденційності та розмежування доступу до даних шляхом використання стандартів криптографічного захисту даних; інтероперабельність, що передбачає перевикористання як даних, наявних в ключових державних реєстрах та зовнішніх системах, так і даних, що вже були надані суб'єктами ЗЕД; незмінність даних, згідно з якими забезпечується фіксація та відстеження історії будь-яких запитів та транзакцій, спрямованих на внесення змін до інформації, електронна ідентифікація користувачів, що вносили зміни в дані, захист від несанкціонованого доступу до інформації, неможливість зміни чи втрати журналів роботи з даними, неможливість зміни інформації та документів, що були надані користувачами із використанням кваліфікованого електронного підпису (КЕП); побудова в усіх інформаційно-комунікаційних системах митних органів комплексної системи захисту або системи управління інформаційною безпекою з підтвердженою відповідністю згідно з вимогами про захист інформації в інформаційно-комунікаційних системах та про забезпечення кібербезпеки.

Варто відзначити, що формування спеціального відомчого законодавства, щодо правового забезпечення кібербезпеки митного простору України, в контексті законодавства загальної дії, здійснюється в розвиток положень Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII (Закон № 2163-VIII) [15], який був прийнятий у відповідь на виклики, пов'язані зі зростанням кіберзагроз, що створюють ризики для національної безпеки.

Норми Закону слугують правовим підґрунтям для дослідження проблем забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

26 серпня 2021 року Президент України Указом «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» № 447/2021 (Стратегія) [16] затвердив довгостроковий документ, з метою забезпечення кібербезпеки, як одного із пріоритетів у системі національної безпеки України. Цей документ прийшов на зміну Указу Президента України від 15 березня 2016 року № 96 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [17], що був першою спробою стратегування державної політики у означеній сфері і який було скасовано, у зв'язку із затвердженням Стратегії.

Стратегія кібербезпеки України базується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року № 2824-IV. На виконання Стратегії та ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України», з метою забезпечення функціонування національної системи кібербезпеки Кабінетом Міністрів України було прийнято Постанову № 1426 від 29 грудня 2021 року «Про затвердження Положення про організаційно-технічну модель кіберзахисту» [18].

Глобальна цифровізація зумовлює кардинальні трансформаційні зміни митної сфери, роблячи її вразливою до нових, іноді унікальних, типів кіберзагроз. Паралельно спостерігається посилення митної кібербезпеки більшості країн світу.

Діджиталізація митного простору України актуалізує ризики посилення кібератак. Серед основних чинників, що сприяють цьому, можна виділити наступні: невідповідність митної інфраструктури сучасним вимогам кібербезпеки, недостатній рівень захищеності митної інформаційної інфраструктури та державних електронних ресурсів, відсутність системного підходу до кіберзахисту та дієвих інструментів убезпечення кіберризиків, недосконалість організаційно-технічної

інфраструктури забезпечення кібербезпеки, а також недостатня ефективність митних органів у протидії кіберзагрозам та слабка координація між суб'єктами митної кібербезпеки.

Для мінімізації ризиків кібератак у митному просторі України необхідно розробити та законодавчо закріпити положення щодо упровадження комплексу заходів в частині: модернізації ІКТ-інфраструктури, тобто, оновлення програмного забезпечення, що використовується в митному просторі України, встановлення сучасних систем захисту інформації, систем раннього виявлення та оповіщення вторгнень, систем захисту від DDoS-атак; підвищення рівня кіберобізнаності суб'єктів, що здійснюють діяльність у митному просторі України. Мова іде, передусім, про регулярні навчання з питань кібербезпеки, ознайомлення з основними загрозами та способами їх запобігання, упровадження політики безпечного використання інформаційних систем; створення та унормування системи моніторингу митних кіберзагроз, яка дозволить оперативно виявляти та реагувати на інциденти; посилення міжнародного співробітництва для активізації співпраці з міжнародними організаціями та іншими країнами в галузі кібербезпеки, обміну досвідом та розробки спільних стратегій протидії кіберзагрозам; залучення приватного сектору до забезпечення кібербезпеки митного простору України, який має досвід у розробці та упровадженні рішень в галузі інформаційної безпеки; розробки, унормування та упровадження системи фінансового убезпечення кіберризиків, передусім, шляхом страхування.

Проведення митної реформи в Україні, в контексті підготовки вступу до ЄС, передбачає упровадження спеціального програмного забезпечення, адже функціонування спільного європейського митного простору забезпечують 17 основних та 16 додаткових систем. В Україні на сьогодні побудовано 2: INCTS (спільний транзит) і ВТІ (зобов'язуючі рішення). Для цього необхідні інвестиції, адже програмне забезпечення має відповідати європейським стандартам. Велика увага приділяється процесу цифровій трансформації Держмитслужби. За програмою Ukraine Facilities передбачено 4,5 млрд євро саме на цю мету. За таких умов, діджиталізація виступає ключовим інструментом для забезпечення балансу між контролем та сприянням законній міжнародній торгівлі. Тому розвиток «е-Митниці» є одним із головних завдань для реформ у митній сфері, які висуває ЄС [19].

Впровадження європейських ІТ-стандартів у митній сфері невіддільне від необхідності проведення комплексної структурної реформи митниці, як головної державної інституції, що здійснює захист економічних інтересів держави шляхом митного контролю та оформлення товарів, що переміщуються через митний кордон України, стягує мині платежі, протидіє контрабанді і порушенню митних правил.

Ключовим аспектом розвитку безпечного митного кіберпростору є проактивна державна політика в галузі митної кібербезпеки. Ця політика повинна забезпечувати постійну адаптацію до мінливого кіберсередовища та сприяти інтеграції національних систем митної кібербезпеки у глобальний світовий контекст, дотримуючись найкращих міжнародних стандартів.

Підпунктом 2 п. 3 ст. 8 Закону № 2163-VIII унормовано, що функціонування національної системи кібербезпеки забезпечується шляхом створення нормативно-правової і термінологічної бази, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу і НАТО.

Водночас актуальним викликом для України залишатиметься на найближчу перспективу адаптація національного законодавства до вимог ЄС. Так, у ЄС 7 січня 2024 року набула чинності Постанова про кібербезпеку (Постанова), в якій окреслено заходи для зміцнення кібербезпеки європейських інституцій, органів та організацій [20]. У Постанові перелічено кроки для запровадження внутрішнього управління з кіберризиків і рамки врядування та контролю для кожної структури ЄС. Документ також передбачає створення нової Міжвідомчої ради з кібербез-

пеки (ІІСВ), яка наглядатиме й підтримуватиме реалізацію Постанови в структурах ЄС. Крім того, Постанова надає розширені повноваження команді реагування на комп'ютерні надзвичайні події в інституціях, органах, офісах і агентствах ЄС (CERT-EU), яка діятиме як хаб для розвідки можливих загроз, обміну інформацією й реагування на інциденти. З огляду на ці повноваження CERT-EU буде перейменована на Сервіс кібербезпеки для інституцій, органів, офісів і агентств ЄС, але абревіатура CERT-EU залишиться чинною. Структури ЄС розроблять внутрішні процеси управління кібербезпекою в межах періоду, визначеного в постанові, і проводитимуть оцінювання ризиків. ІІСВ буде створена й уведена в дію щонайшвидше для стратегічного виконання розпоряджень CERT-EU в межах її розширеного мандата, надання рекомендацій і підтримки структурам ЄС та нагляду за реалізацією Постанови [11, с. 99].

Європейська рада у березні 2021 року визнала необхідність зміцнення кібербезпеки на рівні ЄС та надала політичні рекомендації із забезпечення належного рівня захисту у цій сфері для персоналу, баз даних, комунікаційних мереж, інформаційних систем та для процесу прийняття рішення. У березні 2022 року Єврокомісія представила відповідні законодавчі пропозиції, які були погоджені на рівні Ради ЄС та Європарламенту у червні 2023 року. ЄС затвердила директиву про підтримку високого рівня кібербезпеки «для подальшого підвищення стійкості та потенціалу реагування на інциденти як державного та приватного секторів, так і ЄС загалом». Нова директива ЄС під назвою NIS2 замінила директиву з безпеки мереж та інформаційних систем (Директива NIS [21]). Директива NIS2, яка набула чинності 16 січня 2023 року, повністю замінить чинну Директиву NIS від 17 жовтня 2024 року. NIS2 призначена встановити базовий рівень для заходів контролю над ризиками кібербезпеки у всіх секторах, на які поширюється дія директиви. Директива спрямована на гармонізацію вимог кібербезпеки та реалізацію заходів кібербезпеки у різних державах-членах. Встановлено мінімальні правила для нормативно-правової бази та започатковані механізми ефективної співпраці між відповідними органами в кожній державі ЄС. У той час як у старій директиві NIS держави-члени несли відповідальність за визначення того, які організації мають кваліфікуватися як оператори основних послуг, нова директива NIS2 запровадила загальне правило для ідентифікації організацій, що підпадають під відповідне регулювання. При цьому, в тексті уточняється, що директива не застосовуватиметься до організацій, які провадять діяльність у таких галузях, як оборона чи національна безпека, громадська безпека та правоохоронні органи. Судова система, парламенти та центральні банки також виключені зі сфери дії. NIS2 [22] застосовується до державних адміністрацій на центральному та регіональному рівнях. Держави-члени можуть вирішувати, що це стосується й адміністрацій на місцевому рівні. Крім того, нова директива приведена у відповідність до галузевого законодавства, зокрема, з положенням про цифрову операційну стійкість для фінансового сектора та директивою про стійкість критично важливих об'єктів, щоб забезпечити юридичну ясність та узгодженість між NIS2 та цими актами [11, с. 100].

Отже, всебічне упровадження діджиталізованих митних послуг характеризується наявністю підвищеного ступеню кіберризиків (кіберзагроз) для усіх учасників митних правовідносин (Держмитслужби, митниць, суб'єктів ЗЕД, митних брокерів тощо).

Кіберзагрози є одними з найбільших актуальних викликів для сучасної митної сфери. Наслідки кіберзагроз (тобто, безпосередня реалізація кіберризиків у формі збитків) для митної сфери України можуть бути катастрофічними.

Така небезпека простежується у декількох основних напрямах: 1) збої в роботі митних систем, де кібератаки можуть призвести до зупинки митного оформлення, що характеризуються спричиненням значних збитків для економіки України та порушенням міжнародних торговельних відносин; 2) витік конфіденційної інформації, внаслідок якої хакери можуть отримати доступ до персональних даних гро-

мадян, комерційної таємниці підприємств, що може призвести до порушення прав, репутаційних втрат та фінансових збитків; 3) шахрайство з митним оформленням, коли кібератаки можуть бути використані для незаконного ввезення або вивезення товарів, ухилення від сплати митних платежів, легалізації доходів, отриманих злочинним шляхом тощо; 4) дестабілізація економічної ситуації в цілому, адже, постійні кібератаки можуть створити атмосферу нестабільності та невизначеності у митному просторі України, що відлякуватиме інвесторів та сповільнюватиме загальнонаціональне економічне зростання.

Вказані види ризиків, що характеризуються складною природою, потребують фінансового убезпечення, а процес такого убезпечення – належного нормативного унормування. Актуальність означеної проблеми обумовлена сучасним рівнем прояву негативних наслідків кіберзагроз у митній сфері, недостатнім функціональним потенціалом традиційних засобів у подоланні кіберризиків.

Останніми роками в Україні, аналогічно до більшості держав з розвиненою економікою, для вирішення вказаних проблем активно застосовується кіберстрахування [23, с. 13]. Відсутність належного правового регулювання відносин із кіберстрахування, поряд з непоодинокими спробами страховиків запровадити на ринок страхових послуг пропозиції зі страхування кіберризиків в межах інших, часто несумісних видів страхування, також посилюють актуальність цієї проблематики [23, с. 15].

Одні з перших спроб надання послуг з кіберстрахування, були здійснені в США у 2010 році [24]. Однак, інтерес до поняття «кіберстрахування» з боку вчених-правників та економістів істотно збільшився разом з набранням 24 травня 2016 року чинності Регламентом Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) [26].

Відсутність в Україні спеціального правового регулювання відносин з кіберстрахування (не дивлячись на набуття чинності новим Законом України «Про страхування» від 18 листопада 2021 року № 1909-IX [26]), не заважає окремим страховикам поширювати практику включення до страхових полісів зі страхування майна, транспортних засобів тощо, окремих видів кіберризиків.

Для України, зобов'язання з легалізації механізму кіберстрахування випливають з положень ст. 8 Конвенції Ради Європи № 108 «Про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних» [27], ратифікованої Верховною Радою України 6 липня 2010 року, Конвенції Ради Європи «Про кіберзлочинність» від 21 листопада 2001 року [28] та ст. 15 Угоди про асоціацію.

За загальним правилом, закріпленим у ч. 1 ст. 5 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року № 80/94-ВР, якщо інше прямо не передбачено законом, обов'язок щодо забезпечення захисту інформації в інформаційно-телекомунікаційних системах покладається на їх власників, в порядку та на умовах, визначених у договорі, який укладаються ними із володільцями інформації [29].

Наведена норма має особливе значення для визначення і нормативного закріплення особи страхувальника за договором кіберстрахування, оскільки проводить чітку лінію розмежування обов'язків, щодо захисту ІТС та інформації, яка в них обробляється чи зберігається між власниками таких систем і володільцями інформації [23, с. 19].

За своєю природою кіберризики пов'язані з використанням комп'ютерного обладнання та програмного забезпечення як у (локальних) мережах, так і у мережі Інтернет загалом [30, с. 5].

За таким підходом, до розуміння сутності кіберризиків, на думку вчених, у значенні предмета кіберстрахування можуть розглядатися інформаційно-телекомунікаційні системи, технології, реєстри чи бази даних, а так само інформація, включаючи конфіденційну, що перебуває у володінні суб'єк-

тів господарювання або органів, наділених господарською компетенцією щодо управління цими об'єктами [23, с. 21].

Існування в митній сфері широкої групи кіберризиків, які супроводжують митні процедури та управління ними обумовлено характером протиправних дій та (або) бездіяльності, якими вони спричиняються, а також наслідками їх прояву (збитків) для страхувальників.

Аналіз існуючих нормативних та доктринальних підходів до характеристики кіберризиків та протиправних діянь, які обумовлюють їх виникнення з позицій інтересів страхувальника дозволяє науковцям констатувати, що їх зміст не завжди охоплюється майновою сутністю (отже, не відноситься виключно до майново страхування). Це пов'язано з тим, що як предмет кіберстрахування, інформація, інформаційно-телекомунікаційні системи, технології, бази даних є, передусім, немайновими об'єктами права власності [31, с. 93].

Отже, напрацьовані у науковій літературі особливості кіберстрахування дають підстави розглядати його як окремий вид страхування, що виключає можливість страхування кіберризиків, як похідної складової інших категорій страхових ризиків, визначених Законом України «Про страхування» [23, с. 27].

Зростання митних кіберзагроз та кібератак створює сприятливі умови для розвитку кіберстрахування. Створення ефективних страхових програм митного кіберзахисту дозволяє не лише відшкодувати збитки, завдані кібератаками, але й забезпечити комплексну безпеку митних інформаційних систем.

Кіберстрахування митних кіберризиків є перспективним напрямком розвитку страхового бізнесу. Його розвиток тісно пов'язаний з динамікою кіберзагроз та постійним удосконаленням технологій кібербезпеки. Для подальшого розвитку цього сегмента як митного, так і страхового ринків, необхідно забезпечити належне правове регулювання та розробити сучасні стандартизовані страхові продукти.

Висновки. За результатами проведеного дослідження можна сформулювати наступні науково-теоретичні висновки:

1) пришвидшення та підвищення якості митних процедур забезпечується шляхом спрощення і автоматизації існуючих процесів та зменшення впливу людського фактора. В контексті набуття Україною статусу кандидата у члени ЄС, ІКС митниці мають бути сумісними з аналогічними системами інших країн, передусім із ЄС, що потребує зменшення відмінностей у митних процедурах, забезпечення миттєвого обміну інформацією та вимагає забезпечення високого рівня безпеки електронних ресурсів;

2) належне нормативне забезпечення безпеки митного кіберпростору України на етапі формування спеціального законодавства має відбуватися паралельно за двома пріоритетними векторами, де: за першим – необхідно визначити і унормувати основний категоріально-термінологічний апарат (митна кіберзагроза (митний кіберризик), митний кіберінцидент, митна кібератака тощо), порядок, вимоги та заходи із забезпечення кіберзахисту митного кіберпростору, основні цілі, напрями та принципи державної політики у цій сфері, повноваження державних органів та основні засади координації їхньої діяльності із забезпечення митної кібербезпеки; за другим – необхідно визначити і нормативно врегулювати основні інструменти фінансового убезпечення митного кіберпростору України від потенційних кіберризиків, що можуть завдати значних збитків (шкоди) учасникам митних правовідносин;

3) протягом 2022–2024 років законодавцем прийнято низку нормативно-правових актів, що врегульовують окремі аспекти діджиталізації митної справи, а саме: 1) процедура спільного транзиту; 2) технологічні інструменти: «Єдине вікно для міжнародної торгівлі», «єЧерга», «Електронна митниця»; 3) діджиталізація процедури ввезення гуманітарної допомоги; 4) окремі аспекти діджиталізації митної брокерської діяльності; 5) діджиталізація митної справи тощо. Вищенаведеними окремими прикладами врегулювання різних напрямів діджиталізації митного простору України, доводиться факт практичної реалізації виконання Україною зобов'язань, прийнятих на себе

згідно Угоди про асоціацію в сфері цифрової трансформації митної справи;

4) процеси тотальної діджиталізації митного простору України актуалізують потребу кіберзахисту з метою забезпечення сталості *митного кіберпростору*, як віртуального простору, що надає можливості здійсненню реалізації митних відносин, який утворений внаслідок функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням Інтернет та (або) інших глобальних мереж передачі даних;

5) напрями та орієнтири побудови глобального цифрового митного простору вимагають захисту від кіберзагроз, як наявних та потенційно можливих явищ і чинників, що створюють небезпеку митним інтересам України у митному кіберпросторі, мають негативний та (або) послаблюючий вплив на стан кібербезпеки України та кіберзахист її об'єктів;

6) діджиталізація митного простору України актуалізує ризики посилення кібератак. Серед основних чинників, що сприяють цьому, можна виділити наступні: невідповідність митної інфраструктури сучасним вимогам кібербезпеки, недостатній рівень захищеності митної інформаційної інфраструктури та державних електронних ресурсів, відсутність системного підходу до кіберзахисту та дієвих інструментів убезпечення кіберризиків, недосконаліть організаційно-технічної інфраструктури забезпечення кібербезпеки, а також недостатня ефективність митних органів у протидії кіберзагрозам та слабка координація між суб'єктами митної кібербезпеки;

7) кіберризики, що характеризуються складною природою, потребують фінансового убезпечення шляхом упровадження кіберстрахування митних ризиків, а процес такого убезпечення – належного нормативного унормування.

Список використаної літератури:

1. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27 червня 2014 року. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text.
2. Шевченко Л. В. Адміністративно-правова характеристика діджиталізації у сфері митної справи. Аналітично-порівняльне правознавство. 2022. № 5. С. 318-323. URL: https://app-journal.in.ua/wp-content/uploads/2022/12/61.pdf.
3. Про схвалення Концепції створення багатофункціональної комплексної системи «Електронна митниця»: Розпорядження Кабінету Міністрів Україні від 17 вересня 2008 р. № 1236-р. URL: https://zakon.rada.gov.ua/laws/show/1236-2008-%D1%80#Text.
4. Митний кодекс України: Закон України від 13 березня 2012 року № 4495. URL: https://zakon.rada.gov.ua/laws/show/4495-17#Text.
5. Бліщук К. М. Європейські вектори вдосконалення митної політики в Україні // Економіка і суспільство. Електронний журнал. Вип. 48. 2023. URL: http://www.economyandsociety.in.ua/index.php/journal/article/view/2221/2144.
6. Commission staff working document. Analytical Report following the Communication from the Commission to the European Parliament, the European Council and the Council Commission Opinion on Ukraine's application for membership of the European Union. URL: file:///C:/Users/38067/Desktop/SWD_2023_30_Ukraine.pdf.
7. Іванченко Е. Господарсько-правовий аналіз процесу діджиталізації митної справи: сучасний стан та перспективи розвитку. Сучасні виклики для приватного права України: європеїзація, діджиталізація, війна : матеріали Всеукр. наук.-практ. конф. Київ : НДІ приватного права ім. Ф. Г. Бурчака НАПрН України, 2023. С. 68-78.
8. Іванченко Е. Особливості діяльності митних брокерів в умовах правового режиму воєнного стану: сучасний стан та перспективи правового регулювання. Юридичний вісник. 2023. № 6. С. 26-36.
9. Іванченко Е. П. Інституційні зміни діяльності митних брокерів в умовах правового режиму воєнного стану: особливості та перспективи правового регулювання. Соціальне спрямування економічної діяльності в умовах викликів воєнного стану та повоєнного відновлення в Україні: правові та організаційні проблеми : матеріали наук.-практ. круглого столу (м. Київ, 30 листопада 2023 р.). Київ, НДІ приватного права ім. Ф. Г. Бурчака НАПрН України, 2023. С. 80-91.

10. Вінник О. М. Правове регулювання відносин цифровізації: місце і роль в правовій системі та системі господарського права України. Актуальні проблеми права: теорія і практика. № (43). 2022. URL: https://journals.snu.edu.ua/index.php/app/article/view/361/342.
11. Рєзнікова В., Пацурія Н., Головачова А. Правове забезпечення національної системи кібербезпеки і обороноздатності в сучасних економіко-правових умовах. Право України. 2024. № 4. С. 89-10.
12. Про затвердження Положення про Єдину автоматизовану інформаційну систему митних органів, порядок і умови застосування її систем: Наказ Міністерства фінансів України від 19 травня 2023 року № 263. URL: https://zakon.rada.gov.ua/laws/show/z1132-23#n17.
13. Про реалізацію рішення Комітету з управління інформаційними технологіями у системі управління державними фінансами: Наказ Міністерства фінансів України від 9 лютого 2024 року № 63. URL: https://customs.gov.ua/en/documents/pro-realizatsiiu-rishennia-komitetu-z-upravlinnia-informatsiinimi-tekhnologiiami-u-sistemi-upravlinnia-derzhavnimi-finansami-420.
14. Electronic Customs Multi-Annual Strategic Plan for Customs – 2019 Revision. MASP-C Rev. 2019 Version 1.1. URL: https://taxation-customs.ec.europa.eu/system/files/2019-12/2019_masp_strategic_plan_en.pdf.
15. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
16. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.
17. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 року № 96. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text.
18. Про затвердження Положення про організаційно-технічну модель кіберзахисту: Постанова Кабінету Міністрів України від 29 грудня 2021 року № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text.
19. Відбувся круглий стіл «Українська митниця в умовах вступу України до Європейського союзу». Міжнародний фонд «Відродження». 2 квітня, 2024. URL: https://www.irf.ua/vidbuvsya-kruglyj-stil-ukrayinska-mytnyczya-v-umovah-vstupu-ukrayiny-do-yevropejskogo-soyuzu/.
20. New rules to boost cybersecurity of the EU institutions enter into force. European Commission, 08 January 2024. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6782.
21. On measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive): Directive (eu) 2022/2555 of the European Parliament and of the Council of 14 December 2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555&qid=1674579731975&from=EN.
22. The NIS2 Directive: A high common level of cybersecurity in the EU. European Parliament, 08 February 2024. URL: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333.
23. Пацурія Н. Б., Заярний О. А. Кіберстрахування як засіб забезпечення господарського правопорядку в інформаційній сфері: поняття, механізм та умови реалізації. Право України. 2021. № 7. С. 13–29.
24. Leslie Scism. Insurers Creating a Consumer Ratings Service for Cybersecurity Industry. The Wall Street Journal. 2019. URL: https://www.wsj.com/articles/insurers-creating-a-consumer-ratings-service-for-cybersecurity-industry-11553592600.
25. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679.
26. Про страхування: Закон України від 18 листопада 2021 року № 1909-IX. URL: https://zakon.rada.gov.ua/laws/show/1909-20#Text.
27. Про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних: Конвенція Ради Європи від 28 січня 1981 року № 108. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text.

28. Про кіберзлочинність: Конвенція Ради Європи від 21 листопада 2001 року. URL: https://zakon.rada.gov.ua/go/994_575.
29. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 липня 1994 року. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
30. Розвиток кіберстрахування як сегменту глобального страхового ринку. URL: https://kon-insurance.mnau.edu.ua/files/work_2020/6.pdf.
31. Заярний О. А. Класифікація адміністративних інформаційних правопорушень, як метод наукового дослідження адміністративної деліктності та інструмент удосконалення адміністративно-деліктного законодавства. Адміністративне право і процес. № 4 (10), 2014. С. 80-100.

Ivanchenko E. Topical issues of legal support for cybersecurity and cyber insurance of the customs space of Ukraine: current state and improvement prospects

The article studies legal support for cybersecurity of the customs space of Ukraine amidst modern economic-legal conditions in terms of basic principles of the state customs policy in the area concerned and cyber insurance as an effective financial mechanism for protecting the rights and legitimate interests of participants in customs relations from financial losses that may be caused by customs cyber incidents.

The analysis of the legal doctrine on the issues under study and the customs legislation of Ukraine allowed the author to conclude that the processes of all-encompassing digitalization of the customs space of Ukraine actualize the need for cyber defense to ensure the sustainability of customs cyberspace as a virtual space which provides opportunities for implementing customs relations, which is formed as a result of the functioning of compatible (connected) communication systems and the provision of electronic communications via the Internet and (or) other global networks.

Global digitalization is driving sweeping transformational changes in the customs sector, making it vulnerable to new types of cyber threats. At the same time, customs cybersecurity is being strengthened in most countries.

The digitalization of Ukraine's customs space entails the risks of increased cyberattacks. The author notes that among leading causes are the following: inconsistency of the customs infrastructure with modern cybersecurity requirements, insufficient level of security of the customs information infrastructure and state electronic resources, lack of a systematic approach to cyber defense and effective tools for securing cyber risks, imperfection of the organizational and technical infrastructure for ensuring cybersecurity, as well as underperformance of customs authorities in countering cyber threats and poor coordination between the subjects of customs cybersecurity.

The author proves that a key aspect of the development of a secure customs cyberspace is a proactive state policy on customs cybersecurity. Such policy should ensure continuous adaptation to the changing cyber environment and facilitate the integration of national customs cybersecurity systems into the global context, adhering to the highest international standards.

Based on research findings, the author concludes that customs cyber risks are characterized by a complex nature and require financial security – cyber insurance, and the latter requires proper statutory regulation.

Key words: *customs reform of Ukraine, state customs policy, customs affairs, electronic customs, digital transformation of customs space, customs cyberspace, cybersecurity of customs space, customs cyber risk (cyber threat), cyber insurance of customs risks.*