правоохоронна діяльність митних органів; інші питання, які стосуються технічної реалізації різних митних операцій, тощо.

Деякі автори як недолік МК МС відзначають наявність у ньому норм, які відсилають до положень національного митного законодавства [2, с. 58–60]. Таке викладення нормативного матеріалу ускладнює його вивчення і використання посадовими і приватними особами, оскільки виникає необхідність звернення до норм національного законодавства всіх держав-членів Митного союзу. Також це провокує виникнення колізій у правових нормах і правозастосовчій практиці.

Література:

1. Абрамов, Д. Я. Кучма. Київ : НАДУ, 2009. Ч. 1 : Філософсько-методологічні та системні основи забезпечення національної безпеки.– 248 с.

2. Лазарев Б. М. Компетенция органов управления / Б. М. Лазарев. – М. : Юрид. лит., 1972. – 280 с.

МІЖНАРОДНІ НОРМИ ЩОДО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Блайда М. А.

Студент кафедри міжнародного права та порівняльного правознавства факультету міжнародних відносин Національного авіаційного університету м. Київ, Україна

Найважливішою ознакою глобального розвитку є інформаційне суспільство, фундамент якого становлять новітні технології та засоби комунікації. Будучи «специфічною формою соціальної організації, в якій нові технології генерування, обробки та передачі інформації стали фундаментальними джерелами продуктивності та влади», інформаційне суспільство схильне до особливо складних загроз, оскільки широкий спектр можливостей впливу ІКТ дуже різноманітний і характеризується високим ступенем небезпеки для всіх сфер життєдіяльності соціуму та функціонування держави. У цьому контексті проблема вдосконалення системи державних гарантій конституційних прав людини та громадянина в інформаційній сфері набуває особливої актуальності [1, с. 117].

Рівень розвитку інформаційно-комунікаційних технологій держави є визнаним у міжнародному співтоваристві важливим індикатором оцінки

військово-політичного та соціально-економічного потенціалу держави загалом. Україна у цьому сенсі не є винятком.

Міжнародне право встановлює, що забезпечення права адекватну інформацію є умовою ефективної реалізації всіх інших права і свободи громадян. На основі дотримання конституційних норм щодо недоторканності приватного життя та конфіденційності кореспонденції має будуватися вся система нормативного правового забезпечення безпеки в інформаційній сфері, оскільки права та свободи людини та громадянина мають найвищий пріоритет.

Закономірно, що концептуальні засади та принципи правового регулювання безпеки в інформаційній сфері, розроблені на міжнародному рівні, відповідно до пункту 49 Резолюції 2200А (XXI) Генеральної Асамблеї ООН знаходять більшою чи меншою мірою відображення, як вважає комісія Європейського Союзу з кібербезпеки, законодавстві всіх економічно розвинених країн. Найважливішим стратегічним завданням забезпечення інформаційної безпеки є стан інформаційного простору, в якому виключені можливості порушення прав особистості, суспільства і держави. Конституційно-правова база має створювати підстави для реалізації політики інформаційної безпеки всіх трьох об'єктів: держави, суспільства, особистості «з урахуванням специфіки вимог кожного об'єкта до захисту своїх ресурсів» [2, с. 82].

Експоненційний розвиток інформаційно-комунікаційних технологій стає викликом для національної безпеки в контексті захисту тріади інтересів особистості, суспільства та держави в інформаційній сфері. Неконтрольовані процеси у глобальних мережах та специфіка політичної боротьби у віртуальній сфері прямо та опосередковано впливають на забезпечення захисту національних інтересів. Цей виклик національної безпеки вкрай актуальний у зв'язку зі стихійним створенням відкритих інформаційних мереж загального призначення, їх підключенням до міжнародних телекомунікаційних мереж». Про загрозу національній безпеці будь-якої держави свідчить той факт, що розробка віртуальної міжнародної мережі, забезпечення працездатності та вдосконалення актуальних технологій контролюється Міністерством оборони США[3, с. 54].

Динаміка та характер розвитку інформаційних технологій інтенсифікують новітні виклики та загрози, спрямовані на особистість як уразливий суб'єкт інформаційних відносин, оскільки досягає потенційно-глобальної аудиторії за допомогою піринговых мереж та підключення до мережі Інтернет. Окінавська хартія глобального інформаційного суспільства декларує: «інформаційно-комунікаційні технології є одним із найважливіших факторів, що впливають на формування суспільства двадцять першого століття. Їх революційний вплив стосується способу

життя людей, їхньої освіти та роботи, а також взаємодії уряду та громадянського суспільства. Інформаційно-комунікаційні технології швидко стають життєво важливим стимулом для розвитку світової економіки. Перед усім світом відкриваються великі можливості» [4].

Таким чином, правові підходи, відображені у національних нормативних правових актах країн різноманітні. Однак спільними для всіх держав, які використовують глобальні інформаційні інфраструктури, є проблеми, пов'язані з управлінням інформаційною інфраструктурою, забезпеченням безпеки транскордонної передачі даних, захистом соціальних структур у державі від шкідливого інформаційного впливу, забезпеченням безпеки інформаційної інфраструктури.

Література:

1. Інформаційна безпека держави у контексті протидії інформаційним війнам : навчальний посібник / за заг. ред. В. Б. Толубка. К. : НАОУ. 2004. С. 315.

2. Сопілко І.М. Становлення мережевого суспільства та питання кібербезпеки. Сопілко І.М. *Юридичний вісник. Повітряне і космічне право.* 2016. № 1. С. 79–86.

3. Сулейманова Ш.С., Назарова Е.А. Информационные войны: история и современность : учебное пособие / Сулейманова Ш.С., Назарова Е.А.М. Международный издательский центр «Этносоциум». 2017. С. 90.

4. Окинавская хартия глобального информационного общества. Окинава, 22 июля 2000 года. URL: https://zakon.rada.gov.ua/laws/show/998_163#Text

5. Захист інформаційної безпеки як функція держави. URL: http://www.mego.info/матеріал/23-захист-інформаційноїбезпеки-як-функція-держави