

(корисливим). Як приклад можна навести фіктивне банкрутство, при якому ознакою розмежування виступає суб'єкт злочину (при фіктивному банкрутстві він спеціальний) [7, с. 39].

Підбиваючи підсумки, маємо наголосити на особливій важливості правильної кримінально-правової оцінки вчиненого та належній кваліфікації дій винної особи для забезпечення повноти реалізації кримінального закону на сучасному складному етапі розвитку Українського суспільства.

Список використаних джерел

1. Селецький С. І. Кримінальне право України. Загальна частина: навчальний посібник. Київ : ЦУЛ, 2008. 496 с.
2. Карпович О. Г. Анализ актуальных проблем противодействия законной предпринимательской деятельности в уголовном законодательстве некоторых европейских государств. URL: <https://www.lawmix.ru/comm/771> (дата звернення: 29.04.2020).
3. Коваленко П. М. Ретроспективний аналіз українського та світового досвіду боротьби з шахрайством з фінансовими ресурсами на транснаціональному рівні. *Підприємництво, господарство і право*. 2003. № 6. С. 79-83.
4. Про практику застосування судами законодавства про відповідальність за окремі злочини у сфері господарської діяльності : постанова Пленуму Верховного Суду України від 25.04.2003 № 3. URL: <https://zakon.rada.gov.ua/laws/show/va003700-03> (дата звернення: 29.04.2020).
5. Мойсик В.Р. Відмежування шахрайства з фінансовими ресурсами від інших злочинів у сфері господарської діяльності. *Вісник Верховного Суду України*. 2002. № 4. С. 26-30.
6. Про практику розгляду судами кримінальних справ про виготовлення або збут підроблених грошей чи цінних паперів : постанова Пленуму Верховного Суду України від 12.04.1996 № 6. URL: <https://zakon.rada.gov.ua/laws/show/v0006700-96> (дата звернення: 29.04.2020).
7. Лиманов В. В. Отграничение мошенничества от смежных составов преступлений. *Законность*. 1998. № 3. С. 39-43.

Тульба Н.

*студентки 1 курсу магістратури
юридичного факультету*

Тернопільського національного економічного університету

*Науковий керівник: к.ю.н., доцент кафедри безпеки,
правоохоронної діяльності та фінансових розслідувань ТНЕУ*

Зайцева-Калаурі.В.

МІЖНАРОДНА ІНФОРМАЦІЙНА БЕЗПЕКА

В час розквіту ХХІст. та в процесі глобального «вживлення» інформаційних технологій в усі сфери життєдіяльності людства, питання захисту прав на високотехнологічному рівні являється загостреним, як ніколи. Саме безпека на інформаційному рівні часто є пріоритетною для країни, оскільки визначає, з одного боку, рівень захищеності і стійкості основних сфер функціонування суспільства чи країни щодо небезпечного інформаційного впливу, а з іншого інтенсивність розвитку суспільства в тій чи іншій сфері за рахунок ефективного використання накопичених людством знань [1, с. 41].

Поняття інформаційної безпеки залежно від його використання розглядається з різних сторін. У найзагальнішому вигляді – інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави [2, с.38].

Вплив інформаційної революції та інших високих технологій на прискорену інтеграцію міжнародного співтовариства обумовлюють появу і необхідність вирішення нових проблем, узгодження нових міжнародних принципів взаємодії та правил поведінки учасників міжнародних відносин.

Саме для цього світова спільнота створила необхідні міжнародні акти, задля боротьби з хакерськими атаками на банківські системи та інформаційні системи державної безпеки, інтелектуальним піратством, застосування тарозповсюдження інформаційної зброї, загрозою інформаційних війн і інформаційного тероризму, здатних викликати інформаційні конфлікти зі значними руйнівними наслідками. Одними з таких являються:

- Резолюція ГА ООН 53/576 (1998 р.) «Роль науки і техніки в контексті міжнародної безпеки, роззброєння та інших, пов'язаних з цим сфер»;
- Резолюція ГА ООН 54/49 (1999 р.) «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки»;
- Резолюція ГА ООН 55/28 (2000 р.) «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки»;
- Резолюція ГА ООН 60/45 (2005 р.) «Досягнення у сфері інформатизації і телекомунікацій у контексті міжнародної безпеки» та багато інших.

Міжнародну безпеку слід розглядати як політику, що сприяє створенню ефективних гарантій миру як для окремої країни, так і для всього світового співтовариства. Визнання проблеми інформаційної безпеки на міжнародному рівні обумовлюється такими чинниками глобалізації:

1. У більшості індустріально розвинутих країн проводяться дослідження і розробки нової інформаційної зброї, що дозволяє здійснювати безпосередній контроль над інформаційними ресурсами потенційного противника, а за необхідності прямо впливати на них.

2. Кардинально змінилася оцінка доктрини інформаційної безпеки в цілому і позиції більшості країн світу, які усвідомили вагомість інформаційних загроз і необхідність створення відповідного механізму для контролю інформаційного протиборства[3].

Разом з тим до нових інформаційних видів зброї виявляють інтерес як політичні угруповання, так і терористичні та кримінальні організації, що загрожує новим видом озброєнь, втратою міжнародних ресурсів для вирішення глобальних проблем бідності, стихійних лих, техногенних катастроф, голоду, епідемій тощо. Розуміння цих факторів створює засади теоретичного і практичного обґрунтування так званої системи глобальної соціальної безпеки, побудованої на відкритості і широкому співробітництві[4, с. 652].

Вчені різних країн наголошують, що використання нових інформаційних технологій і засобів впливу високорозвинутих країн на менш технологічні країни світу призвело до зміни глобального і регіонального балансів сили, зумовило нові сфери конфронтації між традиційними і новими центрами глобального протистояння, уможливило досягнення переваг в інформаційних технологіях і засобах маніпулювання суспільною свідомістю для широкомасштабної експансії із застосуванням не обмежених міжнародним правом видів озброєнь.

З-поміж вартих уваги теоретичних поглядів на міжнародну безпеку доцільним є згадати французького теоретика Реймона Арона, який вважав, що безпека у світі незалежних держав може ґрунтуватися або на слабкості суперників (їх повному або частковому роззброєнні), або на власній силі [5]. Зважаючи на глобальність проблеми інформаційної безпеки, розвинуті країни розпочали реалізацію довгострокових державних програм, спрямованих на забезпечення захисту критично важливих інформаційних структур. Під час дискусій та розгляду прикладних аспектів міжнародної інформаційної безпеки було визначено специфіку, істотні характеристики та типологію інформаційних загроз, узгоджено термінологію та зміст основних понять в новій сфері міжнародного співробітництва. Міжнародна інформаційна безпека визначається як взаємодія сторін міжнародних відносин з операцій підтримання сталого миру на основі захисту міжнародної інфосфери, глобальної інфраструктури та суспільної свідомості світової спільноти від реальних і потенційних інформаційних загроз.

Міжнародні інформаційні операції характеризуються як форма міждержавного протиборства, яка реалізується з використанням інформаційного впливу на системи управління різного призначення інших держав, а також на політичну владу і суспільство в цілому, на інфраструктуру і ЗМК для досягнення переваги і кінцевої мети інформаційної операції з одночасним захистом національної інфосфери від аналогічних дій [6].

Одним із специфічних проявів проблематики міжнародної інформаційної безпеки є те, що інформаційні війни, які зараз відбуваються, не тільки підсилюють найрозвиненіші країни, але й дають шанс стати на один рівень із ними країнам колишнього другого і третього світу. Це пов'язано з асиметричним характером інформаційної зброї. Така її властивість дозволяє будь-якій державі в критичний момент вести боротьбу з сильнішим противником. Застосування інформаційної зброї в цьому випадку виявляється найбільш адекватною відповіддю на сторонні агресивні дії. Істотні прояви інформаційних чинників міжнародної безпеки кардинально змінили оцінку доктрини інформаційної безпеки в цілому і позиції більшості країн світу, які усвідомили потенціал інформаційних загроз і необхідність створення відповідного міжнародного механізму для контролю інформаційного протиборства. Аналіз показує, що позиція розвинутих країн визначається пильною увагою до інформації, яка по праву вважається одним з головних факторів володіння сучасним світом, а саме:

- визнання проблеми міжнародної інформаційної безпеки як гіпотетичного силового протистояння;

- перенесення розгляду концепції міжнародної інформаційної безпеки на регіональний або тематичний рівень;

- виділення з комплексної проблеми міжнародної інформаційної безпеки таких складових, як кримінальні та терористичні міжнародні інформаційні загрози і створення міжнародного механізму контролю подібних інформаційних злочинів.

Декілька іншою є позиція країн, які не належать до західної моделі цивілізації. Зокрема, така позиція визначається наступними напрямками:

- надання пропозицій щодо встановлення міжнародно-правової норми про заборону застосування засобів впливу на інформаційні ресурси та інформаційний потенціал міжнародного, регіонального та національного призначення;

- створення спеціального Міжнародного суду з інформаційної злочинності;

- спільні розробки технології глобального захисту від інформаційної агресії.

Список використаних джерел

1. Богуш В. М., Юдін О. К. Інформаційна безпека держави. К.: МК-Прес. 2005. 432 с.
2. Юдін О.К. Інформаційна безпека держави: Навчальний посібник. Х.: Консум. 2005. 576 с.
3. Л.В.Борисова, В.В.Тулупов, Харківський національний університет внутрішніх справ, ISSN 1727-1584. ПРАВО І БЕЗПЕКА 2013. № 1 (48).
4. Макаренко Є. А., Рижиков М. М., Ожеван М. А., Головченко В. І., Гондюл В. П. Міжнародна інформаційна безпека: Сучасні виклики та загрози. К.: Центр вільної преси. 2006. 916 с.
5. АронРаймон. Мемуары: 50 лет размышлений о политике. Memoires: 50 AnsdeReflexionPolitique / Р. Арон; пер. с фр. Г.А. Абрамова, Л.Г. Ларионовой М.: Ладомир. 2002. 873 с.
6. Гриняев С. Экспертыкорпорации «РЭНД» об информационной стратегии. URL: <http://attend.to/commi> (дата звернення: 18.04.2020).