УДК 659
DOI: 10.5281/zenodo.4127228

Л.В. Борисова, к.ю.н., доцент, НУЦЗ України, м. Харків

О.В. Закора, к.т.н., старший викладач, НУЦЗ України, м. Харків

А. Б. Фещенко, к.т.н, доцент, НУЦЗ України, м. Харків

Borysova L., Ph.D in Law sciences, Associate Professor,
National University of Civil Protection of Ukraine, Kharkiv

O.B. Zakora, Ph.D in Technical Sciences. senior lecturer,
National University of Civil Protection of Ukraine, Kharkiv

A.B. Feshchenko, Ph.D in Technical Sciences, Associate Professor
National University of Civil Protection of Ukraine, Kharkiv

КОНЦЕПТУАЛЬНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

CONCEPTUAL PRINCIPLES OF INFORMATION SECURITY

Показано, що зростаючий вплив сучасних інформаційних і комунікаційних чинників на розвиток суспільно-політичних відносин в суспільстві вимагає уніфікації норм з правового регулювання міжнародної інформаційної безпеки. Показано, що у сучасних умовах інформаційна безпека держави потребує комплексного осмислення

Ключові слова: *інформація, комунікації, інформаційні впливи, інформаційні загрози, інформаційна безпека.*

It is shown that the growing influence of modern information and communication factors on the development of socio-political relations in society requires the unification of norms on the legal regulation of international information security. It is shown that in modern conditions the information security of the state needs a comprehensive understanding

Keywords: *information, communications, information influences, information threats, information security.*

Постановка проблеми. Процеси, що відбуваються в суспільному житті, можна охарактеризувати як посилення ролі та значення інформації як у суспільстві в цілому, так і в житті кожної окремої людини зокрема. Інформація отримує реальне матеріально-енергетичне, соціально-економічне, політичне і вартісне вираження. За цих умов одним з першочергових завдань, що постають перед правовою державою, є вирішення протиріччя між реально існуючими і зростаючими потребами особистості, суспільства і держави в якісних інформаційних ресурсах, продуктах та послугах і необхідністю забезпечення їх інформаційної безпеки. Політика у сфері інформаційної безпеки спрямована на досягнення такого рівня духовного та інтелектуального потенціалів країн, який є достатнім для розвитку державності і соціального прогресу.

Аналіз останніх досліджень і публікацій. При написанні статті використані праці українських науковців. Проблему інформаційної безпеки відображено у працях А. Марущака, В. Петрика, В. Ліпкана, Б. Кормича, В. Почепцова, Р. Лук'янчук та інші фахівці як складову національної безпеки, її невід'ємний компонент. Поза увагою науковців залишились проблеми побудови в державі інформаційного суспільства як органічного сегмента глобального інформаційного співтовариства.

Постановка завдання. Метою статті є аналіз інформаційної безпеки на міжнародному рівні та створення умов для побудови в державі інформаційного суспільства як органічного сегмента глобального інформаційного співтовариств.

Виклад основного матеріалу. Визнання проблеми інформаційної безпеки на міжнародному рівні обумовлюється такими чинниками глобалізації: у більшості розвинутих країн проводяться дослідження і розроблення нової інформаційної зброї, що дозволяє здійснювати безпосередній контроль над інформаційними ресурсами потенційного противника, а в необхідних випадках впливати на них; кардинально змінилася оцінка 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. Політичні дискусії на Міжнародному семінарі з проблем інформаційної безпеки (Женева, 1999 р.), який відбувся під егідою Інституту ООН з дослідження проблем роззброєння (*UNIDIR – United Nations institute for disarmament research*) за участю департаменту з питань роззброєння Секретаріату ООН та представників понад 50 країн світу, підтвердили актуальність проблеми та своєчасність її розгляду в рамках ООН. У визначенні підходів до її вирішення виявилися різні позиції, котрі відповідали стратегічним інтересам учасників дискусії. Позиція розвинутих країн передбачала визнання проблеми міжнародної інформаційної безпеки як: гіпотетичного силового протистояння; перенесення 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.

Позиція країн, які не належать до західної моделі цивілізації, передбачала такі пропозиції: 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; спільне розроблення технології глобального захисту від інформаційної агресії.

Женевська зустріч виявила стратегічну проблему міжнародної інформаційної безпеки – проблему домінування в глобальній інформаційній сфері

із застосуванням інформаційних озброєнь, тобто прагнення до контролю значних територій та соціумів, проблему інформаційного дисбалансу сил міжнародного світопорядку.

Концепція міжнародної інформаційної безпеки визначає критичні структури, які у першу чергу зазнають впливу в умовах інформаційного протиборства. Найбільш вразливими вважаються політична, суспільна, економічна, військова, науково-технологічна, духовна сфери життєдіяльності суспільства, а саме:

– у політичній сфері інформаційна безпека стосується структур підготовки та прийняття політичних рішень, структур управління місцевої та регіональної влади, структур виборчих систем, інформаційно-телекомунікаційних урядових систем спеціального призначення;

– для економічної сфери критичними вважаються системи загальноекономічного аналізу та прогнозування економічного розвитку, структури прийняття рішень та координації управлінських дій в економічній сфері, зокрема, в умовах надзвичайного стану, інфраструктури банківських мереж і систем, системи управління в критично важливих для функціонування держави структурах (енергетика, транспортні комунікації, телекомунікаційні та інформаційні мережі);

– у військовій сфері вразливими в умовах інформаційного протиборства вважаються інформаційні ресурси збройних сил, військово-промисловий комплекс, системи управління військами, системи контролю і постійного спостереження, канали надходження інформації стратегічного, оперативного, тактичного, розвідувального характеру;

– глобальними загрозами в науково-технологічній сфері є феномен транскордонного переміщення інтелектуальних ресурсів, тобто вивезення інформації унікального науково-технологічного характеру на біологічних носіях до міжнародних систем спостереження, аналізу і прогнозування тенденцій науково-технологічного розвитку в різних країнах з метою доступу до об’єктів критичної інфраструктури, до конфіденційних баз і банків даних;

– суспільна сфера є найбільш вразливою для інформаційних впливів, оскільки включає системи формування громадської думки, структури засобів масової комунікації, інформаційно-організаційні структури політичних партій, громадських рухів, плюралізму і незалежності виявлення поглядів, вільного обміну думками, ідеями та інформацією;

– духовна сфера стає критичною в умовах конфесійного протистояння, релігійного фанатизму, трансформації духовних ідеалів та морально-етичних цінностей.

Інформація, як глобальне явище, утворює глобальні проблеми в міжнародній інформаційній сфері, складовим елементом якої є національна інформаційна сфера, яку кожна країна намагалася регулювати відповідно до своїх правових традицій, звичаїв та суспільної моралі. Інформаційна безпека як чинник міжнародних відносин, вплив якої має універсальний характер на поведінку багатьох акторів міжнародних відносин. До того ж трансформація самої сутності понять проблеми безпеки після закінчення «холодної війни» і розпаду біполярної міжнародної системи, потребує концептуального перегляду принципів функціонування міжнародних та національних інститутів, що відповідають за безпеку, а також врахування в нових доктринах інформаційної складової міжнародної безпеки.[1][1] Зважаючи на глобальність складових інформаційної безпеки, розвинуті країни світу розпочали реалізацію довгострокових державних програм, спрямованих на забезпечення захисту критично залежних від інформації структур.

У 1996 р. проблему міжнародної інформаційної безпеки було винесено на політичний та міжнародно-правовий рівень: Концепцію міжнародної інформаційної безпеки було обговорено на міжнародній конференції з проблем становлення інформаційного суспільства та глобальної цивілізації (ПАР, 1996 р.); у спільному комюніке зустрічі на найвищому рівні США-Російська Федерація у 1997 р. було підкреслено загрозу створення інформаційної зброї і визнано наявність воєнної складової глобального процесу інформатизації; на

[1] Міжнародна інформаційна безпека: Сучасні виклики та загрози. – К. : Центр вільної преси, 2006. – С. 9.

52-ій сесії Генеральної Асамблеї ООН прийнято Резолюцію 53/70 від 4 грудня 1998 р., в якій зазначалося, що міжнародна спільнота визнає проблему інформаційної безпеки як багатоаспектний стратегічний напрям взаємодії держав у світі. Було запропоновано ООН розглянути конкретну типологію інформаційних загроз, визначити критерії цієї проблеми, включаючи розробку міжнародних принципів безпеки глобальних інформаційних систем та внести пропозиції до комплексної доповіді[2].[2]

Міжнародна інформаційна безпека визначається як взаємодія акторів 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[3].[3]

Інформаційна безпека, як поняття в міжнародних відносинах залежно від його використання розглядається у декількох ракурсах. У найзагальнішому вигляді – інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави[4].[4]

Інформаційна безпека включає в себе сукупність організаційних, соціально-економічних, правових заходів, спрямованих на забезпечення стабільності розвитку суспільства і держави та цивілізації.

Стратегії глобального інформаційного протиборства лежать в основі аналітичних розробок дослідницьких інституцій різних країн світу, метою яких є саме забезпечення інформаційного лідерства у сфері міжнародної безпеки. За результатами досліджень аналітики виділяють такі моделі системи глобальної інформаційної безпеки:

Модель А – створення абсолютної системи захисту країни-інформаційного лідера проти будь-якого виду наступальної інформаційної зброї, що обумовлює об'єктивні переваги в потенційній інформаційній війні,

---

[2] Міжнародна інформаційна безпека: Сучасні виклики та загрози. – К. : Центр вільної преси, 2006. – С. 13-14.
[3] Раймон А. Мемауры: 50 лет размышления о политике / Раймон А. Memoires: 50 Ands de Reflexion Politique ; пер. с фр. Г.А. Абрамова, Л.Г. Лариновой.– М. : Ладомир, 2002.– 873с.
[4] Юдін О.К. Інформаційна безпека держави : навч. посіб. / О.К.Юдін, В.М. Богуш. – Х. : Консум, 2005. – С. 38.

змушує інші країни шукати альянсу у військово-інформаційних діях з країною-інфолідером.

Модель B – створення значної переваги державами-потенційного ініціатора інформаційної війни в наступальних видах озброєнь, у знешкодженні систем захисту державами-протиника засобами інформаційного впливу, координація дій із союзними державами з використаннями визначених засобів інформаційної зброї для ідентифікації джерел і типів інформаційних загроз.

Модель C – наявність кількох країн-інфолідерів та потенційного протиборства між ними, визначення фактору стримування експансії інформаційних загроз, забезпечення в перспективі домінування однієї з держав у сфері міжнародної інформаційної безпеки з можливостями значного впливу на глобальну інфосферу та переважного права вирішення проблем глобального світопорядку.

Модель D – всі конфліктуючі сторони використовують транспорантність інформації для формування ситуативних альянсів, для досягнення переваг локальних рішень, які спроможні заблокувати технологічне лідерство, для використання можливостей інфоінфраструктури на окремих територіях з метою організації внутрішнього конфлікту між опозиційними силами(політичні, сепаратистські, міжнаціональні конфлікти) для проведення міжнародних антитерористичних інформаційних операцій.

Модель E – протиборство світової спільноти та міжнародної організованої злочинності, здатної контролювати перебіг політичних, економічних, суспільних і, зрештою, цивілізаційних процесів. Можливість такої моделі передбачена в дослідженні Національної ради розвідки США «Mapping the global future»- 2020 у версії «Коло страху» («Cycle of fear»), яка є найбільш песимістичним сценарієм майбутнього світової спільноти[5].[5]

Концепція міжнародної інформаційної безпеки визначає критичні структури, які зазнають впливу в умовах інформаційного протиборства.

---

[5] Міжнародна інформаційна безпека: Сучасні виклики та загрози. — К.:Центр вільної преси, 2006. – С. 147.

Найбільш вразливими вважаються політична, суспільна, економічна, військова, інноваційна, науково-технологічна, духовна сфери життєдіяльності суспільства.

В економічній сфері критичними є системи загальноекономічного аналізу та прогнозування економічного розвитку, структури прийняття рішень та координації управлінських дій в економічній сфері, зокрема, в умовах надзвичайного стану, системи управління в критично важливих для держави структурах(енергетика, комунікації, інформаційні мережі).

Феномен інформаційної безпеки в міжнародних відносинах обумовлюється стратегічною спрямованістю інформаційних впливів проти критично важливих структур життєдіяльності і функціонування міжнародного співтовариства. Міжнародна інформаційна безпека – стан міжнародних відносин, який виключає порушення світової стабільності та створення загрози безпеці держав і світової спільноти в інформаційному просторі.

Усі питання забезпечення інформаційної безпеки держави, крім технічних засобів захисту інформації, повинні регулюватися нормами міжнародного права, так як засоби інформаційного впливу мають деструктивні наслідки не тільки для держави, проти якої вони спрямовані, а й для всієї світової спільноти.

Загрози інформаційній безпеці реалізуються через порушення критичної інфраструктури, вільного обігу інформації, неправомірні дії щодо інформації, через невідповідність інформаційної політики, засобів інформування громадськості. Відповідно до критичних сфер міжнародного співробітництва класифікуються загрози для інформаційної безпеки. Існують різні типології загроз, але, узагальнюючи, можна виділити такі види загроз: інформаційно-технологічні; інформаційно-комунікаційні; інформаційно-психологічні.

Відповідно міжнародна інформаційна безпека включає такі спрямування:

І. Глобальна інформаційна безпека: безпека розвитку міжнародної інформаційної сфери; захист міжнародного інформаційного ринку від незаконних посягань акторів міжнародних інформаційних відносин; захист та обмеження обігу інформації в цілях глобальної інформаційної безпеки; захист міжнародної інформаційної інфраструктури; захист міжнародних

інформаційних ресурсів; побудова глобального інформаційного суспільства тощо;

II. Інформаційна безпека окремих держав у міжнародному інформаційному просторі: безпека інформаційного простору держави від інформаційних загроз, інформаційних операцій, інформаційного тиску та інформаційних війн з боку інших акторів міжнародних інформаційних відносин; захист державного інформаційного ринку від незаконних посягань акторів міжнародних інформаційних відносин; захист та обмеження міжнародного обігу інформації в цілях державної інформаційної безпеки; побудова та забезпечення належного функціонування інформаційного суспільства;

III. Інформаційна безпека установ у міжнародному інформаційному просторі: захист інформації з обмеженим доступом, яка належить установі, від несанкціонованих дій з боку інших акторів міжнародної інформаційної сфери; доступ до загальнодоступної інформації та інформації, доступ до якої не може бути обмежено; захист від випадкового чи навмисного втручання в нормальний процес функціонування автоматизованої інформаційної системи організації (установи) з боку інших акторів міжнародної інформаційної сфери тощо;

IV. Інформаційна безпека людини в міжнародному інформаційному просторі: захист інформаційної і комунікаційної приватності (особливо персональних даних); вільний доступ до масової та суспільно-значущої інформації; захист від негативного інформаційного впливу; захист інформаційних і комунікаційних прав на міжнародному рівні тощо.

Основними пріоритетами державної політики в інформаційній сфері є забезпечення: захисту інформаційного суверенітету держави, особливо захисту національного інформаційного простору з інформаційним ресурсом і системи формування масової суспільної свідомості; рівня інформаційної достатності для прийняття рішень державними органами, підприємствами і громадянами. З метою забезпечення єдиного підходу щодо захисту державних інформаційних ресурсів створюється окрема підсистема для телекомунікаційного забезпечення функціонування Єдиного веб-порталу органів виконавчої влади. Оптимізації

дій щодо недопущення реалізації загроз інформаційним ресурсам держави необхідно здійснювати проведення оцінювання (аудиту) стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, зокрема тих, що мають доступ до мережі Інтернет.

Висновки. 1. Міжнародна інформаційна безпека – стан міжнародних відносин, який виключає порушення світової стабільності та створення загрози безпеці держав і світової спільноти в інформаційному просторі. 2. Сьогодні світова спільнота приходить до думки про необхідність створення міжнародних актів, які містили б уніфіковані норми з правового регулювання міжнародної інформаційної безпеки. 3. Важливо підкреслити те, що метою інформаційної політики держави є створення умов для побудови в державі інформаційного суспільства як органічного сегмента глобального інформаційного співтовариства, забезпечення пріоритетного розвитку інформаційних ресурсів та інфраструктури, впровадження новітніх інформаційних технологій, захисту національних моральних і культурних цінностей, забезпечення конституційних прав на вільний доступ до інформації. 4. Державна політика визначається пріоритетністю національних інтересів і має на меті унеможливлення реалізації загроз для інформації.

Список використаних джерел

1. Міжнародна інформаційна безпека: Сучасні виклики та загрози. – К. : Центр вільної преси, 2006. – С. 9.

2. Міжнародна інформаційна безпека: Сучасні виклики та загрози. – К. : Центр вільної преси, 2006. – С. 13-14.

3. Раймон А. Мемауры: 50 лет размышления о политике / Раймон А. Memoires: 50 Ands de Reflexion Politique ; пер. с фр. Г.А. Абрамова, Л.Г. Лариновой.– М. : Ладомир, 2002.– 873с.

4. Юдін О.К. Інформаційна безпека держави : навч. посіб. / О.К.Юдін, В.М. Богуш. – Х. : Консум, 2005. – С. 38.

5. Міжнародна інформаційна безпека: Сучасні виклики та загрози. – К.:Центр вільної преси, 2006. – С. 147.

References

1. International Information Security: Current Challenges and Threats. – Kyiv: Center for Free Press, 2006. – P. 9.

2. International Information Security: Current Challenges and Threats. – Kyiv: Center for Free Press, 2006. – P. 13-14.

3. Raymond A. Memoirs: 50 years of thinking about politics / Raymond A. Memoires: 50 Ands de Reflexion Politique; lane. with fr. НА. Абрамова, Л.Г. Larinova. – M .: Ladomir, 2002.– 873 p.

4. Yudin OK Information security of the state: textbook. way. / OK Yudin, VM Bogush. – H.: Konsum, 2005. – P. 38.

5. International Information Security: Current Challenges and Threats. – Kyiv: Center for Free Press, 2006. – P. 147.