СЕКЦІЯ 4
ПРАВО ТА ІНСТИТУТИ ЄВРОПЕЙСЬКОГО СОЮЗУ, ЩО РЕГУЛЮЮТЬ ТРАНСКОРДОННЕ СПІВРОБІТНИЦТВО

УДК 327. 5+351.746/1

Є. А. Макаренко*, д. політ. н., проф.,*
провідний науковий співробітник
відділу трансатлантичних досліджень
ДУ «Інститут всесвітньої історії НАН України»
(Україна, м.Київ)

Політико-правове регулювання сфери міжнародної інформаційної безпеки

У статті проаналізовано програмно-інституціональне забезпечення інформаційної безпеки на рівні міжнародних та регіональних інституцій, з'ясовано засади регуляторної політики щодо протидії глобальним інформаційним загрозам та представлено оцінку переговорного процесу в рамках ООН щодо Міжнародної конвенції з інформаційної безпеки.

Ключові слова: міжнародні організації, міжнародна інформаційна безпека, інституційні засади, регуляторна політика, ООН, Міжнародна конвенція з інформаційної безпеки.

Makarenko E. Political and legal regulation of international information security. *In the article are described the political and legal aspects of information security of international and regional institutions, defined principles of regulatory policy on counteraction global information threats and presented evaluation of the negotiation process under the UN International Convention on Information Security.*

Keywords: international organizations, international information security, institutional framework, regulatory policy, UN, International Convention on Information Security.

Політико-правове регулювання сфери міжнародної інформаційної безпеки є важливим напрямом співробітництва провідних акторів міжнародних відносин на глобальному, регіональному та національному рівнях. До системи політико-правових документів, які регулюють міжнародне інформаційне співробітництво у сучасному світі, відносять загальні (універсальні) та спеціальні принципи і норми, зафіксовані, зокрема, у конвенціях, міжнародних договорах та угодах, резолюціях, деклараціях і рекомендаціях, статутах, актах та директивах міжнародних організацій та у двосторонніх документах. Важливими для розуміння проблеми регулятивного виміру міжнародної інформаційної безпеки є базові принципи міжнародного права, зафіксовані у Статуті ООН і дотичних універсальних документах, що становлять основу права збройних конфліктів, міжнародного гуманітарного права, політико-правових інструментів щодо протиборства з міжнародним тероризмом тощо.

До основних принципів, які стосуються міжнародних інформаційних відносин і, зокрема, міжнародної інформаційної безпеки, відносять: принцип суверенної рівності держав у сфері використання інформаційних ресурсів, забезпечення інформаційного суверенітету держави та рівноправної участі у переговорних процесах щодо встановлення і кодифікації міжнародно-правових документів у сфері інформаційної безпеки; принцип невтручання у внутрішні справи інших держав, який передбачає неприпустимість інформаційної інтервенції і втручання за допомогою інформаційних ресурсів та засобів у внутрішні справи держав з метою проведення спеціальних інформаційних кампаній, ворожої пропаганди та поширення деструктивної чи спеціально спрямованої інформації;

принцип заборони застосування сили або загрози силою, який забороняє використання інструментів інформаційного впливу проти територіальної цілісності чи політичної незалежності будь-якої держави (за винятками використання сили згідно з мандатом Ради Безпеки ООН відповідно до Статті 42 у випадку самооборони, а також Статті 51, яка визнає невід'ємне право кожної держави на самооборону проти збройного нападу з використанням озброєнь нового покоління; принцип мирного врегулювання міжнародних спорів, який зобов'язує держави до превентивної дипломатії або переведення збройного конфлікту на переговорний рівень за допомогою інструментів інформаційного впливу; принцип територіальної цілісності та непорушності кордонів, який стосується визначення меж національного інформаційного простору та заходів захисту від несанкціонованого втручання ззовні; принцип дотримання фундаментальних прав і свобод людини, який визначає конституційні та спеціальні норми, а також норми міжнародних договорів щодо свободи слова та вільного обігу інформації, незалежності і плюралізму міжнародних мас-медіа, свободи вираження, заборони цензури та захисту конфіденційності інформаційних ресурсів; принцип самовизначення народів і націй, який встановлює права національних меншин на культурну самобутність та інформаційну діяльність; принцип міжнародного співробітництва, який зобов'язує держави співробітничати задля зміцнення миру та міжнародного взаєморозуміння, розвитку глобальної інфраструктури з метою досягнення політичних, економічних і соціокультурних інтересів людства[1].

Формування нової геостратегічної структури міжнародних відносин під впливом глобалізації та

швидкоплинного розвитку високих технологій зумовило нові підходи ООН та окреслення нових параметрів міжнародного співробітництва у сфері інформаційної безпеки. Багатогранність інформаційно-комунікаційних технологій у політичному, економічному, безпековому, соціальному та культурному плані, визнання руйнівного чинника нових технологічних озброєнь змусило ООН та інші впливові міжнародні організації включити проблему міжнародної інформаційної безпеки у сферу своїх інтересів та нормотворчої діяльності. В контексті діяльності ООН та інших міжнародних форумів глобального і регіонального характеру по виробленню міжнародно-правового режиму у сфері міжнародної безпеки можна було б звернутися до вже наявних прецедентів: маються на увазі прийняті міжнародні договори і конвенції у високотехнологічних галузях (Договір про принципи діяльності держав по дослідженню і використанню космічного простору, включаючи Місяць і інші небесні тіла, 1967 року, Конвенція по морському праву 1982 року і ін.), а також у військовій сфері (Договір про нерозповсюдження ядерної зброї від 1 липня 1968 року, Договір про обмеження систем ПРО від 26 травня 1972 року, Конвенція про заборону хімічної зброї (набула чинності 29 квітня 1997 року), Конвенція про заборону біологічної зброї (набула чинності 26 березня 1975 року), Конвенція про заборону застосування, накопичення запасів, виробництва і передачі протипіхотних мін і про їх знищення від 18 вересня 1997 року). Як зазначається у політико-правових документах міжнародних організацій, сучасна міжнародна безпека є визначеною системою міжнародних відносин держав з метою підтримання міжнародного миру і стабільності, що регламентується принципами і нормами статуту ООН. Ця система охоплює: 1)

основні принципи міжнародного права; 2) процедури мирного вирішення спорів; 3) спільні дії та миротворчі операції для попередження загрози миру; 4) повноваження ГА ООН та Ради Безпеки ООН з питань роззброєння та обмеження озброєнь [2].

Усвідомлення необхідності суворого дотримання принципів незастосування сили, невтручання у внутрішні справи держав, забезпечення фундаментальних прав і свобод, невикористання високих технологій з протиправною метою, невідповідність міжнародних інформаційних відносин Статуту ООН зумовило розгляд проблеми міжнародно-правового регулювання інформаційної безпеки і встановлення міжнародного контролю за інформаційними озброєннями. Передбачалося з'ясувати позиції світового співтовариства щодо проблеми потенційного воєнного використання інформаційно-комунікаційних технологій для вдосконалення існуючих і створення нових систем озброєнь; визначити основні поняття у сфері міжнародної інформаційної безпеки; розглянути можливість створення міжнародної системи моніторингу інформаційних загроз; розробити міжнародно-правовий режим інформаційної безпеки. Конструктивне обговорення проблеми визначило пріоритети ООН щодо інформаційної безпеки, зокрема, було підкреслено, що в інформаційній сфері необхідна кодифікація спеціальних принципів і норм, що склалися на основі Статуту ООН, і досягнення нових угод, щоб упорядкувати і стабілізувати відносини держав, спрогнозувати їх подальший розвиток, а також інших відносин, пов'язаних з проблемою інформаційної безпеки, зокрема, політичних, соціальних, економічних, гуманітарних, екологічних тощо. Як свідчить політико-правова діяльність міжнародної організації, упродовж 1998-2013 рр. питання міжнародної інформаційної безпеки

постійно обговорювалось на ГА ООН з метою розробки відповідного міжнародного документу на основі ухвалених резолюцій, в яких зафіксовано глобальність проблеми інформаційної безпеки, наявність тісного зв'язку між її різними аспектами, такими, як сталий розвиток, боротьба з бідністю, зміцнення демократичного управління, подолання цифрового розриву тощо. Так, на сесії ГА ООН 4 грудня 1998 року була прийнята резолюція «Досягнення у сфері інформатизації і телекомунікації в контексті міжнародної безпеки», в якій містилися положення про подвійну природу досягнень науки і техніки як у цивільній, так і у воєнній сферах, про застосування новітніх досягнень у модернізації сучасних озброєнь, зокрема, зброї масового ураження, про здатність досягнень науки і техніки здійснювати негативний вплив на міжнародну безпеку [3]. Зважаючи на необхідність регулювання передачі новітніх технологій подвійного призначення, у резолюції було запропоновано встановити жорсткі обмеження на експорт новітніх матеріалів, обладнання та технологій у країни, що розвиваються, для використання у мирних цілях. Виклики високих технологій для міжнародної безпеки у XXI ст., враховуючи неможливість їх вирішення однією або кількома державами, зумовили необхідність проведення багатосторонніх переговорів на рівні ООН та ухвалення резолюцій про міжнародну інформаційну безпеку. Політична дискусія з питань міжнародної інформаційної безпеки засвідчила різні позиції країн, що стосуються бачення потенційних загроз в інформаційних озброєннях та їх використанні проти критично важливих сфер життєдіяльності суспільства. Перш за все йшлося про встановлення міжнародно-правового режиму у сфері інформаційної безпеки, необхідність розробки та ухвалення

концепції міжнародної інформаційної безпеки, принципів, спрямованих на посилення безпеки глобальних і телекомунікаційних систем, попередження інформаційного тероризму і злочинності, створення спеціального міжнародного суду зі злочинів в інформаційній сфері. Принципи розглядалися як робочий варіант кодексу поведінки держав у міжнародному інформаційному просторі, основа для міжнародних переговорів під егідою ООН з цієї проблематики. П'ять базових принципів міжнародної інформаційної безпеки визначають роль і права, зобов'язання і відповідальність держав у міжнародному інформаційному просторі, заходи, спрямовані на обмеження загроз у сфері міжнародної інформаційної безпеки, а також роль ООН у міжнародному співробітництві в контексті цієї проблеми. Так, принцип 1 проголошує, що діяльність кожної держави та інших суб'єктів міжнародного права в міжнародному інформаційному просторі повинна сприяти загальному соціальному та економічного розвитку і здійснюватися таким чином, щоб відповідати завданням підтримання сталого миру і безпеки, захисту суверенних прав інших держав, інтересам безпеки, принципам мирного врегулювання спорів та конфліктів, незастосування сили, невтручання у внутрішні справи, поваги до прав і свобод людини. Така діяльність повинна відповідати праву кожного шукати, отримувати та поширювати інформацію та ідеї, як це зафіксовано у документах ООН, з врахуванням того, що таке право може бути обмежене законом з метою захисту інтересів національної безпеки кожної держави. При цьому кожна держава та інші суб'єкти міжнародного права повинні мати рівні права на захист своїх інформаційних ресурсів та критично важливих структур від неправомірного використання; несанкціонованого інформаційного втручання і можуть

сподіватися на підтримку світового співтовариства в реалізації цих прав. Принцип 2 підкреслює, що держави повинні прагнути до обмеження загроз у сфері міжнародної інформаційної безпеки і з цією метою утримуватися від розробки, створення і використання засобів впливу і завдання шкоди інформаційним ресурсам і системам іншої держави; спрямованого інформаційного впливу на критично важливі структури іншої держави; інформаційного впливу з метою руйнування політичної, економічної та соціальної системи інших держав і задля дестабілізації суспільства; несанкціонованого втручання в інформаційно-телекомунікаційні системи та інформаційні ресурси, їх неправомірне використання; дій, що сприяють домінуванню і контролю в інформаційному просторі; протидії доступу до новітніх ІКТ, створення умов технологічної залежності у сфері інформатизації як загрозу іншим державам; заохочення дій міжнародних терористичних, екстремістських і злочинних угрупувань, що загрожують інформаційним ресурсам та критично важливим структурам інших держав; розробки та ухвалення планів, доктрин, які передбачають ведення інформаційних воєн, здатних спровокувати гонку озброєнь, а також викликати напруженість у відносинах між державами і самих інформаційних воєн; використання ІКТ проти основних прав і свобод людини, які реалізуються в інформаційній сфері; транскордонного поширення інформації, яка суперечить принципам і нормам міжнародного права, а також внутрішньому законодавству конкретних країн; маніпулювання інформаційними потоками, дезінформації та засекречування інформації з метою викривлення психологічного і духовного середовища суспільства, ерозії традиційних культурних, моральних та етичних і естетичних цінностей; інформаційної

експансії, монополії в національних інформаційних системах інших держав, включаючи умови їх функціонування в міжнародному інформаційному просторі. Принцип 3 встановлює, що ООН та її спеціалізовані установи сприятимуть міжнародному співробітництву, метою якого є обмеження загроз у сфері міжнародної інформаційної безпеки і формування відповідної міжнародно-правової бази для визначення ознак та класифікації інформаційних воєн; визначення ознак і класифікації інформаційних озброєнь і засобів відповідного призначення; обмеження обігу інформаційних озброєнь; заборони розробки, поширення і використання інформаційної зброї; попередження загрози виникнення інформаційної війни; визнання безпеки застосування інформаційної зброї щодо критично важливих структур як зброї масового ураження; створення умов для рівноправного і безпечного міжнародного інформаційного обміну на основі загальновизнаних норм і принципів міжнародного права; попередження використання інформаційних технологій і засобів впливу на суспільну свідомість з метою дестабілізації суспільства і держави; розробки процедури взаємного інформування та попередження транскордонного несанкціонованого інформаційного впливу; створення системи міжнародного моніторингу для відстеження загроз в інформаційній сфері; створення міжнародної системи сертифікації технологій і засобів інформатизації і телекомунікацій (в тому числі програмно-технічних) щодо гарантій їх інформаційної безпеки; створення механізму контролю виконання умов режиму міжнародної інформаційної безпеки; створення механізму врегулювання конфліктних ситуацій у сфері інформаційної безпеки; розвитку систем міжнародної взаємодії правоохоронних органів з попередження і

припинення правопорушень в інформаційному просторі; гармонізації на добровільній основі національних законодавств для забезпечення міжнародної інформаційної безпеки. Принцип 4 визначає, що держави та інші суб'єкти міжнародного права повинні нести міжнародну відповідальність за діяльність в інформаційному просторі, яка здійснюється ними, під їхньою юрисдикцією або в рамках міжнародних організацій, членами якої вони є, і за відповідність такої діяльності принципам, які містяться у цьому документі. Принцип 5 стверджує, що будь-які спори між державами та іншими суб'єктами міжнародного права, які виникають при застосуванні цих принципів, регулюються за допомогою встановлених процедур мирного врегулювання спорів [3].

Політико-правові дискусії з проблематики міжнародної інформаційної безпеки виявили різні підходи країн до проблем інформаційної безпеки і зумовили ухвалення ГА ООН резолюції 56/121 (2001 р.) «Боротьба зі злочинним використанням інформаційних технологій», в якій було запропоновано різні заходи боротьби з тероризмом у зв'язку з використанням терористичними та злочинними угрупованнями високих технологій, зокрема, удосконалення національних законодавств у сфері боротьби з кіберзлочинністю; співробітництво правоохоронних органів у разі транскордонного злочинного використання ІКТ; обмін інформацією щодо проблем боротьби зі злочинним використанням ІКТ; правовий захист конфіденційності, цілісності і доступності даних; захист комп'ютерних систем від несанкціонованого втручання; покарання за неправомірне зловживання ІКТ; режим взаємодопомоги у розслідуванні злочинів з ІКТ; інформування громадськості щодо попередження злочинів; вдосконалення ІКТ

з превентивною складовою; необхідність захисту основних прав і свобод приватного життя. Керуючись цими пріоритетами і враховуючи, що проблеми інформаційної безпеки пов'язані із сучасними формами тероризму, ГА ООН також ухвалила резолюцію 57/239 (2003 р.) «Створення глобальної культури кібербезпеки», до преамбули якої увійшли посилання на попередні резолюції з міжнародної інформаційної безпеки і боротьби зі злочинним використанням ІКТ, що підкреслює багатогранність проблеми інформаційної безпеки і наявність тісного зв'язку між її різними аспектами. В основу концепції глобальної культури кібербезпеки покладено усвідомлення комплексної взаємозалежності, яка існує в сучасному світі інформаційних засобів і технологій, множинності акторів, що діють у цій сфері, і розуміння неможливості забезпечення кібербезпеки на даному етапі лише за рахунок прийняття державою суто технологічних або правоохоронних заходів. У резолюції «Створення глобальної культури кібербезпеки», зокрема, йдеться про те, що кібербезпека залежить не тільки від дій державних чи правоохоронних органів, а й превентивних заходів і підтримки всього світового співтовариства. У додатку «Елементи для створення глобальної культури кібербезпеки» міститься перелік «складових», на основі яких має забезпечуватися безпека мереж – від етики і демократії до відповідальності, реагування, оцінки ризиків та управління безпекою – і які сприятимуть державам-членам ООН у розробці міжнародно-правової бази інформаційного суспільства. За наполяганням США, пріоритетом позиції якої є проблема боротьби з міжнародним тероризмом в усіх аспектах міжнародного співробітництва, зокрема, боротьби з кібертероризмом, інформаційною злочинністю та безпеки

комп'ютерних мереж, ГА ООН ухвалила резолюцію 567/27 «Заходи з ліквідації міжнародного тероризму» (2003 р.), у якій підкреслюється важливість розгляду проблеми в рамках ООН, засуджуються прояви тероризму та їх згубні наслідки для суспільств у різних країнах світу, підкреслюється, що боротьба держав з тероризмом має здійснюватися згідно зі Статутом ООН, нормами міжнародного права і відповідними міжнародними конвенціями, пропонується терміново розробити проект міжнародної конвенції з ліквідації тероризму і стверджується провідна роль ООН та її спеціалізованих установ у попередженні терористичних загроз різного характеру, зокрема, усіх форм інформаційного тероризму (медіа, кібер, психотероризму, лінку, чіпінгу, фішингу тощо) [4-6].

Проблема неухвалення документу з міжнародної інформаційної безпеки на 60 сесії ГА ООН пов'язана з неузгодженістю політичних позицій групи урядових експертів (до неї увійшли представники 15 держав, зокрема РФ, Китаю, США, Франції, Великої Британії, Йорданії, Білорусії, Малі, Малайзії, Мексики, Кореї, ПАР – голова групи представник РФ А.В.Крутських) з таких питань, як практичні заходи з попередження розробки, виробництва, використання та поширення інформаційних озброєнь в рамках глобального режиму міжнародної інформаційної безпеки. Загальні параметри такого режиму, запропоновані на основі пропозицій РФ, охоплюють відмову від розробки, створення і використання інформаційних озброєнь; спрямованого нападу за допомогою інформаційних озброєнь на інші держави; несанкціонованого втручання в інформаційні системи та критично важливі та неправомірного їх використання, монополії в міжнародному інформаційному просторі; протидії доступу до новітніх ІКТ-

технологій, створення технологічної залежності у сфері ІКТ від інших держав, заохочення терористичних, екстремістських та злочинних угруповань до використання інформаційних озброєнь, розробки планів та доктрин ведення інформаційних воєн, інформаційної експансії (маніпулювання, викривлення, порушення основних прав і свобод, встановлення контролю над інформаційно-комунікаційними структурами) тощо. До міжнародного договору передбачалося увести положення про ознаки і класифікацію інформаційних озброєнь та дотичних засобів; заходи з обмеження обігу інформаційних озброєнь (розробки, виробництво, застосування); заходи з попередження загрози інформаційних воєн, визнання інформаційних озброєнь зброєю масового ураження, забезпечення свободи міжнародних інформаційних потоків, попередження використання інформаційних озброєнь терористичними угрупованнями, механізм контролю, моніторингу, спостереження та вирішення конфліктних ситуацій, координація правоохоронних дій держав, сертифікацію ІКТ та гарантії їх інформаційної безпеки, гармонізацію міжнародного права та національних законодавств з міжнародної інформаційної безпеки. Серед заходів для зміцнення інформаційної безпеки в глобальному масштабі було запропоновано національним урядам, експертам аналітичних центрів, силовим структурам ООН здійснити компетентний аналіз проблем у сфері інформаційної безпеки на міжнародному рівні, визначити основні критерії щодо безпеки інформації і телекомунікацій або незаконного використання цих систем за допомогою Інтернет, розробити міжнародні принципи безпеки інформаційних та телекомунікаційних систем світу в контексті боротьби з тероризмом та торгівлі конфіденційною інформацією,

враховуючи, що такі технології можуть бути використані для дестабілізації безпеки держав, впровадити у військовій та оборонній сфері телекомунікаційні системи на основі новітніх досягнень технологій інформаційної безпеки [7].

Упродовж сесій ГА ООН (2007-2013 рр.), держав-члени міжнародної організації інформували Генерального Секретаря ООН про свою політико-правову оцінку загальних проблем інформаційної безпеки, про заходи на національному рівні для зміцнення інформаційної безпеки і сприяння міжнародному співробітництву в цій сфері, про зміст відповідних міжнародних концепцій, спрямованих на безпеку глобальних інформаційних і телекомунікаційних мереж, та про заходи на рівні міжнародного співтовариства, які б забезпечували інформаційну безпеку на глобальному рівні. Відтак, аналіз переговорного процесу в рамках ООН, зважаючи на політичні позиції держав-членів, засвідчив необхідність продовження консультативного і переговорного процесів з міжнародної інформаційної безпеки як унікальної ініціативи, спрямованої на забезпечення міжнародного миру і стабільності у найбільш широкому контексті, з урахуванням інформаційних загроз військово-політичного, злочинного і терористичного характеру.

Джерела:

1. Міжнародна інформаційна безпека: сучасні виклики та загрози / [Макаренко Є.А., Гондюл В.П., Рижков М.М. та ін.]. – К.: Центр вільної преси, 2006. – 916с.

2. Макаренко Є.А. Міжнародне співробітництво у сфері інформаційної безпеки: регіональний контекст// Актуальні проблеми міжнародних відносин, Випуск,102, Ч.1, 2011. – с. 32-46

3. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности. Резолюция A/RES/53/70 ГА ООН [Электронный ресурс]. – Режим доступа: http://daccess-ods.un.org/TMP/4475585.html

4. Борьба с преступным использованием информационных технологий. Резолюция A/RES/56/121 ГА ООН [Электронный ресурс]. – Режим доступа: http://daccess-ods.un.org/TMP/8467463.html

5. Создание глобальной культуры кибербезопасности. Резолюция A/RES/57/239 ГА ООН [Электронный ресурс]. – Режим доступа: http://daccess-ods.un.org/TMP/8353689.html.

6. Меры по ликвидации международного терроризма. Резолюция A/RES/58/81 ГА ООН [Электронный ресурс]. – Режим доступа: http://daccess-ods.un.org/TMP/5449476.html.

7. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности [Электронный ресурс]. – Режим доступа: http:// un.org