УДК 323.28:007+351.746:007:341.123

ФАНЬ ЧЖОЖАНЬ

Міжрегіональна Академія управління персоналом, м. Київ

ПРАВОВІ ГАРАНТІЇ ПРОТИДІЇ ІНФОРМАЦІЙНОМУ ТЕРОРИЗМУ І РОЗВИТОК СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ДІЯЛЬНОСТІ ООН

Наукові праці МАУП, 2012, вип. 3(34), с. 168–173

Проблема міжнародної безпеки вже неодноразово порушувалась багатьма країнами — членами ООН як одна з найважливіших та актуальних у процесі сучасного світового розвитку та міжнародної співпраці як на регіональному, так і на глобальному рівні.

Особливого значення набуває процес розробки і формування наукового забезпечення діяльності щодо створення цілісної і комплексної міжнародної програми глобальної інформаційної безпеки. Оскільки ж ключовим механізмом реалізації такої програми є саме система міжнародного права, то пріоритетна роль у науковій розробці і запровадженні на практиці програми забезпечення міжнародної інформаційної безпеки належить саме науці міжнародного права. При цьому вельми важливим видається надання першочергової уваги тим об'єктивним небезпекам, які на сьогодні постали перед міжнародною спільнотою. Однією з них є загроза інформаційного тероризму на міжнародному рівні, про що вже неодноразово наголошувалось під час роботи Генеральної Асамблеї ООН.

Дослідження правових гарантій протидії міжнародному тероризму і розвитку системи інформаційної безпеки у діяльності ООН зумовлюється кількома важливими причинами. По-перше, глобалізація інформаційних зв'язків перетворила загрозу інформаційного тероризму з регіональної на глобальну, що несе в собі потенційну загрозу дестабілізації усій світовій спільноті. Таким чином, створення надійної системи гарантій протидії цьому небезпечному явищу є одним з пріоритетних та найактуальніших завдань, що постали в ході міжнародної співпраці. По-друге, наявність розривів у рівні розвитку різних держав робить їх більш або менш захищеними від такого різновиду небезпеки, як інформаційний тероризм, боротьба з яким потребує акумуляції значних інформаційних, телекомунікаційних, технічних та інтелектуальних ресурсів. Це спричиняє нерівність у протистоянні подібній загрозі, що, в свою чергу, накладає зобов'язання на розвинені держави сприяти створенню глобальної системи інформаційної безпеки, в якій би кожна держава (незалежно від рівня свого розвитку на наявних у її розпорядженні ресурсів) почувалась захищеною рівною мірою з іншими. По-третє, численні дискусії, що виникали між різними державами — членами ООН під час спільних обговорень проблем інформаційного тероризму та інформаційної безпеки, переконливо засвідчили наявність різних позицій та різних методологічних підходів щодо розв'язання цього комплексу питань. Це зумовлює актуальність пошуку консенсусу насамперед на науковій основі, що дасть можливість зняти суперечності між тими чи іншими конкретними державами і запропонувати універсальний підхід (що дасть підстави розробити комплексну міжнародну систему заходів протидії інформаційному тероризму), заснований на спільних цінностях міжнародної безпеки і розвитку, що поділяються всіма без винятку державами — членами ООН.

Отже, досліджуючи правові гарантії протидії міжнародному тероризму в аспекті розвитку системи інформаційної безпеки у діяльності ООН, ми маємо вирішити такі конкретні завдання: а) визначити правовий зміст загрози інформаційного тероризму і механізми протидії цій небезпеці на міжнародному рівні; б) встановити значення протидії інформаційному тероризму в системі глобальної інформаційної безпеки; в) охарактеризувати правові міри протидії інформаційному тероризму, що пропонувались певними державами — членами ООН (насамперед Китаєм).

Важливим правовим кроком у напрямі визнання загрози інформаційного тероризму як глобального явища стали результати проведення 56 сесії Генеральної Асамблеї ООН, коли було прийнято резолюцію "Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки" № 56/19, у якій чітко зазначено, що поширення і використання інформаційних технологій та засобів стосується інтересів усього міжнародного співтовариства. Утім, як було зафіксовано у резолюції ООН, ці технології та засоби потенційно можуть бути використані з метою дестабілізації міжнародної безпеки як у воєнній, так і в цивільній сферах, спричинити поширення на міжнародному рівні такого явища, як інформаційний тероризм [1]. Водночас було наголошено, що навіть з огляду на те, що інформаційні технології сприяють вільному потоку інформації, демократизації суспільства та економічному прогресу, не можна не визнати, що існують потенційні загрози неправомірного та несанкціонованого використання інформаційних технологій у різних сферах життєдіяльності держав, що створює загрозу для міжнародної безпеки. Оцінюючи зміст міжнародних концепцій про безпеку глобальних інформаційних технологій, було підкреслено, що, незважаючи на ефективність міжнародного співробітництва у сфері інформаційної безпеки, кожна держава має право і несе відповідальність за захист власних інформаційних ресурсів та інформаційних систем. Існуючі ризики мають транскордонний характер, і будь-які превентивні заходи, спрямовані на обмеження потенційних втрат від злочинного чи терористичного нападу, зокрема, і для міжнародної безпеки, повинні здійснюватися з урахуванням захисту інформаційно-телекомунікаційних ресурсів та систем. Фактично це означало міжнародне визнання того факту, що саме ООН має бути основним форумом з обговорення проблем міжнародної інформаційної безпеки та протидії міжнародному тероризму [2].

При цьому під час обговорення в ООН цієї резолюції викристалізувались кілька важливих позицій, які були згодом враховані. Насамперед було вказано, що міжнародна спільнота повинна офіційно відмовитись від виробництва інформаційних озброєнь або оснащення ними своїх збройних сил у найближчому майбутньому паралельно з розробкою системи універсальних критеріїв оцінки проблеми інформаційної безпеки, визначенням основних понять у цій сфері, конкретизацією міжнародних правових гарантій протидії інформаційному тероризму і кіберзлочинності. Результатом цього стало те, що інформаційне озброєння було визнано такою самою загрозою, як і зброя масового ураження. При цьому було зазначено, що всі досягнення у сфері науки і техніки можуть бути використані з протиправною метою, а отже, ця проблема є глобальною і для розвинених у технічному відношенні країн, і для країн, що розвиваються. Ще одним важливим кроком у створенні систем інформаційної безпеки та протидії інформаційному тероризму стало введення у міжнародно-правовий обіг такого поняття як інформаційна колонізація. Нагадаємо, що в попередніх документах ООН застосовувались лише такі терміни, як: несанкціоноване втручання, проникнення, санкціоноване втручання, несанкціоноване використання інформації, протиправне використання інформації, інформаційні ресурси, інформаційна зброя, інформаційна війна, інформаційний тероризм, електронні кіберзлочини, кібернетичні злочинці, технологічно передові держави тощо. Це новий феномен інформаційної колонізації було охарактеризовано як "дії однієї держави або держав проти інших з метою встановлення монополії та контролю в інформаційній сфе-

рі, попередження доступу до новітніх технологій або встановлення технологічної залежності в інформаційній сфері, акти інформаційної експансії і встановлення монополії над національними ІКТ, інфраструктурами іншої держави з метою створення умов залежності і контролю". Одним з результатів роботи цієї сесії стало створення спеціальної групи урядових експертів держав — членів ООН для вивчення проблеми міжнародної інформаційної безпеки, зокрема, з'ясування реальних та потенційних загроз у сфері інформаційного тероризму і спільних заходів з їх попередження, визначення заходів, спрямованих на зміцнення безпеки глобальних мереж і систем.

Утім, слід вказати на те, що у тому ж 2001 р. було ухвалено ще одну резолюцію під назвою "Боротьба зі злочинним використанням інформаційних технологій", у якій було запропоновано різні заходи боротьби з інформаційним тероризмом у зв'язку з використанням терористичними та злочинними угрупованнями високих технологій, зокрема, вдосконалення національних законодавств у сфері боротьби з кіберзлочинністю; співробітництво правоохоронних органів у разі транскордонного злочинного використання інформаційно-телекомунікаційних систем; обмін інформацією щодо проблем боротьби зі злочинним використанням інформаційно-телекомунікаційних систем; правовий захист конфіденційності, цілісності і доступності даних; захист комп'ютерних систем від несанкціонованого втручання; покарання за неправомірне зловживання інформацією; режим взаємодопомоги у розслідуванні злочинів, що пов'язані з інформаційним тероризмом; інформування громадськості щодо попередження інформаційних злочинів [3]. Уже в наступному році, посилаючись на попередні резолюції з питань ролі науки і техніки в контексті міжнародної безпеки, підкреслюючи значний прогрес у розробці та впровадженні високих технологій, 57 сесія Генеральної Асамблеї ООН підтвердила важливість проблеми міжнародної інформаційної безпеки й ухвалила Резолюцію № 57/53 про необхідність обговорення існуючих та потенційних загроз у сфері інформаційної безпеки, можливі заходи з їх попередження, а також дослідження міжнародних концепцій на рівні урядових експертів з цієї проблеми. Також було визначено зміст організаційно-практичних заходів щодо розробки проекту міжнародної конвенції з інформаційної безпеки, які стосуються узгодження політичного аспекту у сфері міжнародної інформаційної безпеки, визначення чинників, що впливають на стан міжнародної інформаційної безпеки з урахуванням загроз воєнного, цивільного, терористичного та злочинного характеру, виокремлення узгоджених заходів з попередження використання інформаційних технологій у терористичних цілях, обмеження використання інформаційних озброєнь, координації дії правоохоронних органів з попередження інформаційної агресії, аналіз проблеми координації національних законодавств з проблеми інформаційної діяльності, оцінка можливостей допомоги країнам — жертвам інформаційної агресії.

При цьому найважливішим аспектом інформаційної безпеки було визнано боротьбу із кіберзлочинністю та інформаційним тероризмом, забезпечення захисту інформаційної інфраструктури, особливо її критично важливих сегментів, а також створення глобальної культури кібербезпеки. Враховуючи, що проблеми інформаційної безпеки тісно пов'язані з сучасними формами тероризму, Генеральна Асамблея ООН у розвиток резолюцій про "Досягнення ІКТ у контексті міжнародної безпеки" також ухвалила резолюцію № 57/239 "Створення глобальної культури кібербезпеки", до преамбули якої увійшли посилання на попередні резолюції з міжнародної інформаційної безпеки і боротьби зі злочинним використанням інформаційно-телекомунікаційних систем [4]. Таким чином, в основу концепції глобальної культури кібербезпеки було 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. Мультисуб'єктність, притаманна інформаційним процесам, означає, що в глобальному інформаційному суспільстві власниками і користувачами інформаційних ресурсів, у тому числі критичних, стають не лише органи державної влади і державні інститути, а й приватні підприємства, організації, окремі користувачі, які також розробляють інформаційні системи і мережі, керують ними або обслуговують їх. Роль останніх у справі забезпечення кібербезпеки значно зростає, звідси і необхідність вжиття превентивних заходів щодо зміцнення безпеки у своєму сегменті кіберпростору. У резолюції "Створення глобальної культури кібербезпеки" безпосередньо йшлося про те, що кібербезпека залежить не тільки від дій державних чи правоохоронних органів, а й превентивних заходів й підтримки усього світового співтовариства.

Також у 2003 р. ООН було ухвалено резолюцію № 567/27 "Заходи з ліквідації міжнародного тероризму", у якій підкреслювалась важливість розгляду проблеми в рамках ООН, засуджувались прояви тероризму та їх згубні наслідки для суспільств у різних країнах світу, підкреслювалось, що боротьба держав з тероризмом має здійснюватися згідно зі Статутом ООН, нормами міжнародного права і відповідними міжнародними конвенціями, пропонувалось терміново розробити проект міжнародної конвенції з ліквідації тероризму і стверджувалась 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) [5]. Наступні 58 та 59 сесії Генеральної Асамблеї ООН закликали держави-члени сприяти розробці міжнародних документів у сфері міжнародної безпеки з метою включення цих норм до національних законодавств і регулювання міжнародних відносин в інформаційній сфері. В обговоренні було підкреслено, що наукові та технологічні розробки потребують міжнародного контролю за їх поширенням, оскільки можуть бути застосовані як в мирних, так і воєнних цілях, водночас підтримуючи вільний розвиток науки та вільний обмін науковою інформацією. Стверджувалося, що проблемним є забезпечення вільного доступу до новітніх технологій в інформаційній сфері в умовах необхідності інформаційної безпеки та запобігання тероризму, оскільки саме воєнний аспект використання інформаційно-телекомунікаційних технологій виступає першочерговим і найбільш вагомим за потенційними наслідками застосування інформаційних озброєнь.

Однак 60 сесія Генеральної Асамблеї ООН, попри пропозиції групи урядових експертів ухвалити проект міжнародної конвенції з інформаційної безпеки, ухвалила лише резолюцію № 60/45 "Досягнення у сфері інформатизації і телекомунікацій у контексті міжнародної безпеки", де було підкреслено необхідність продовження багатосторонніх консультацій щодо існуючих та потенціальних інформаційних загроз та створення міжнародних концепцій щодо безпеки глобальних інформаційних та телекомунікаційних систем. Проблема неухвалення документа з міжнародної інформаційної безпеки на 60-й сесії була 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) з таких питань, як: практичні заходи з попередження розробки, виробництва, використання та поширення інформаційних озброєнь в рамках глобального режиму міжнародної інформаційної безпеки. Загальні параметри цього режиму охоплюють відмову від розробки, створення і використання інформаційних озброєнь; спрямованого нападу за допомогою інформаційних озброєнь на інші держави; несанкціонованого втручання в інформаційні та критично важливі системи та неправомірного їх використання, монополії в міжнародному інформаційному просторі; протидії доступу до новітніх інформаційних технологій, створення технологічної залежності у сфері інформації і телекомунікації від інших держав, заохочення терористичних, екстремістських та злочинних угруповань до використання інфор-

маційних озброєнь, розробки планів та доктрин ведення інформаційних воєн, інформаційної експансії (маніпулювання, викривлення, порушення основних прав і свобод, встановлення контролю над інформаційно-комунікаційними структурами) тощо. Водночас до міжнародного договору передбачалося ввести 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, гармонізацію міжнародного права та національних законодавств з міжнародної інформаційної безпеки [6].

Під час проведення 61 сесії Генеральної Асамблеї ООН серед заходів для зміцнення інформаційної безпеки і протидії інформаційному тероризму 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, упровадити у військовій та оборонній сфері телекомунікаційні системи на основі новітніх досягнень технологій інформаційної безпеки.

При цьому варто привернути особливу увагу до позиції Китаю (КНР) в обговоренні цього питання, який запропонував закріпити на офіційному рівні норму, що використання інформаційних технологій має відповідати цілям статуту ООН та основним принципам міжнародних відносин, серед яких є: гарантування безперешкодного потоку інформації з врахуванням національного суверенітету і безпеки та поваги до історичних, культурних і політичних традицій різних країн; права кожної країни на використання власного кіберпростору на основі національного законодавства; активізація міжнародного співробітництва у сфері інформації для подолання асиметрії інформаційного розвитку країн та використання переваг новітніх технологій для економічного зростання. Також Китай підтримав ідею створення під егідою ООН групи урядових експертів для проведення досліджень щодо загроз і проблем у сфері інформаційної безпеки та вироблення відповідної міжнародної політики регулювання, наголошуючи, що міжнародне співробітництво є необхідною умовою, оскільки кіберзлочинність не визнає кордонів, і боротися з нею традиційними методами неможливо [7]. Особливий наголос у позиції Китаю було зроблено щодо безпеки інформаційної інфраструктури з огляду на те, що проблема інформаційної безпеки включає не тільки ризики, пов'язані з уразливістю і взаємозалежністю мереж, а й різні політичні, економічні, військові, соціальні, культурні та багато інших проблем, що зумовлюються зловживанням інформаційними технологіями. Фактично позиція Китаю полягала в тому, що саме ООН є провідним міжнародним форумом для вивчення шляхів вирішення проблеми інформаційної безпеки в сучасному світі, оскільки в межах організації відбулися дискусії щодо поглибленого і всебічного дослідження загроз і проблем у сфері інформаційної безпеки в усіх її аспектах і пошуку ефективних рішень. Більше того, протягом 2007–2011 рр. уряд Китаю розширив свої інвестиції в інформаційну сферу і реалізував програми формування інформаційного суспільства та інформаційної безпеки.

Отже, підбиваючи загальний підсумок проведеному дослідженню, можна сформулювати такі висновки. По-перше, одним з головних завдань у частині протидії міжнародному інформаційному тероризму в контексті формування загальної системи міжнародної

безпеки є кодифікація питань, пов'язаних із забезпеченням міжнародної інформаційної безпеки, і прогресивний розвиток відповідних норм міжнародного права, вироблення і прийняття проекту загального правового документа щодо міжнародної інформаційної безпеки. По-друге, принциповою позицією Китаю щодо проблеми протидії інформаційному тероризму, висловленою під час проведення сесій ООН, був наголос на необхідності розробки проектів багатосторонніх договорів і конвенцій про запобігання неправомірного використання інформаційно-комунікаційних технологій проти глобальної і національної інформаційної інфраструктури та про боротьбу з інформаційним тероризмом. Така позиція видається слушною, з огляду на те, що наразі проблеми інформаційного тероризму мають вирішуватись не стільки на регіональному, скільки на глобальному рівні, що зумовлено самою специфікою загрози міжнародного інформаційного тероризму.

Література

1. *Достижения* в сфере информатизации и телекоммуникаций в контексте международной безопасности. Резолюция A/RES/56/19 ГА ООН. — [Электронный ресурс]. — Режим доступа: http://daccess-ods.un.org/TMP/4296577.html

2. *Рове С. Э.* Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Доклад Первого комитета A/56/533. — [Электронный ресурс]. — Режим доступа: http://daccess-ods.un.org/TMP/7202971.html

3. *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

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

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

6. *Технологический* прогресс и своевременные международные отношения: Учебник / А. В. Крутских, А. В. Торкунов, В. В. Ничков и др.; Под общ. ред. А. В. Крутских. — М.: Просвещение, 2004. — С. 72–74.

7. *Достижения* в сфере информатизации и телекоммуникаций в контексте международной безопасности. Доклад Генерального секретаря A/62/98. — [Электронный ресурс]. — Режим доступа: http://daccess-ods.un.org/TMP/3624342.html

Визначено основні правові гарантії та напрями протидії міжнародному інформаційному тероризму в контексті розробки ефективної міжнародної правової політики забезпечення інформаційної безпеки. Узагальнено матеріал щодо діяльності ООН у цій сфері у XXI ст., схарактеризовано зміст та значення резолюцій ООН з гарантування інформаційної безпеки.

Определены основные правовые гарантии и направления противодействия международному информационному терроризму в контексте разработки эффективной международной правовой политики обеспечения информационной безопасности. Обобщен материал о деятельности ООН в этой сфере в XXI ст., охарактеризованы содержание и значение резолюций ООН по обеспечению информационной безопасности.

The main areas of legal guarantees and countering to the international information terrorism in the context of developing an effective international legal information security policy are identified. The materials on UN activities in this area in the XXI century, describes the content and significance of the UN resolutions on information security are generalized.

Надійшла 20 січня 2012 р.