УДК004.056:341 (045)

МІЖНАРОДНО-ПРАВОВІ ЗАХОДИ ЩОДО УПЕРЕДЖЕННЯ ЗЛОЧИННОСТІ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ШИРОКОВА-МУРАРАШ Ольга Геннадіївна,
кандидат історичних наук, доцент,
Інститут міжнародних відносин Національного авіаційного університету

АКЧУРІН Юрій Равільович,
старший викладач,
Інститут міжнародних відносин Національного авіаційного університету

У статті досліджується проблема міжнародно-правового упередження кіберзлочинності та кібертероризму як результату негативного впливу інформаційних технологій на суспільство.

Ключові слова: *інформаційні телекомунікаційні технології, кібертероризм, кіберзлочинність, інформаційна безпека, інформаційна війна, резолюції ООН.*

Постановка проблеми. Сучасний світ не можливо уявити без інформативно-комунікативних технологій (далі - ІКТ), які трансформували не лише принципи і форми збору, обробки та передачі інформації, вони почали здійснювати могутній вплив на культурний, економічний, політичний, військово-стратегічний аспекти суспільного життя. Разом з тим ІКТ стали одним із основних факторів забезпечення та підтримки стабільного розвитку, а кількість, технічний рівень та доступність інформаційних ресурсів часто визначають рівень розвитку країни та її статус у світовому співтоваристві. У той же час стрімкий розвиток ІКТ в останні десятиріччя обумовив не лише перехід національних інфраструктур на принципово новий рівень розвитку та функціонування, але призвів до виникнення принципово нових загроз системам національної та міжнародної безпеки и породив цілий комплекс негативних геополітичних наслідків.

Ці загрози пов'язані преш за все з можливістю використання ІКТ у цілях, несумісних із завданням підтримки міжнародної стабільності і безпеки, додержання принципів незастосування сили, невтручання у внутрішні справи держав, поваги прав і свобод людини.

Особливу занепокоєність викликає можливість розробки, застосування та розповсюдження інформаційної зброї, виникнення у зв'язку з цим загрози інформаційних війн та інформаційного тероризму, чиї руйнівні наслідки можна прирівняти до наслідків застосування зброї масового знищення.

У геополітичних масштабах ІКТ перетворюються на важливий стимул розвитку військового потенціалу країн за рахунок підвищення їх інформаційної забезпеченості. З'являється можливість використання інформаційного потенціалу розвинутими у науково-технічному відношенні країнами для пригнічування та підкорення собі держав менш розвинутих і, відповідно, більш слабких. У свою чергу це неминуче веде до прискорення поляризації світу, що породжує нестабільність, виникнення та розвитку реальних та потенційних конфліктів, у тому числі загальносвітового й військового значення.

Метою даної статі є висвітлення небезпеки безконтрольного використання інформативно-комунікативних технологій та визначення шляхів нормативного регулювання питань міжнародної інформаційної безпеки.

Вперше занепокоєність можливими наслідками використання всесвітньої інформаційної мережі була висловлена футурологом Елвіном Тофлером у 1993 році, коли широка публіка ще мало що знала про Інтернет. Тофлер вже тоді передбачав, що терористи будуть намагатися здійснити удар по інформаційній та телекомунікаційній інфраструктурі Сполучених Штатів. З цих пір було проведено декілька десятків тисяч досліджень і думки експертів з приводу нового поняття «кібертероризм» полярно поділилися. Перші б'ють тривогу з приводу небезпеки потенційного «електронного Перл-Харбору», інші, як правило, у наукових роботах, регулярно нагадують першим, що до сьогодення у світі не було зареєстровано жодного кібертерористичного акту. До такого висновку прийшов у своїй доповіді «Кібертероризм: міф чи реальність?» Седрик Тевне: «Якщо мистецтво інформаційного піратства відверто викладається в інженерних академіях, університетах, обговорюється на симпозіумах місцевими та міжнародними експертами з питань оборони…, то кібертероризму, у суворому змісті цього слова, не існує й до сьогодні» [1, с. 45].

Але серйозні приводи для занепокоєності все ж таки існують. Сьогодні терористи активно використовують Інтернет для розповсюдження своєї пропаганди на вебсайтах, форумах і у формі відеороликів, перш за все для повідомлення про свої успіхи та залучення прихильників. В історії Інтернету є низка випадків руйнування з політичними цілями стартових сторінок веб-сайтів (зокрема військових чи урядових). Відомі й кібератаки, що мали на меті перевантаження серверів і блокування доступу до них. Як правило це є результат зусиль любителів чи груп фанатиків і поки що не спричинили крупного матеріального, фінансового й тим більш людських втрат.

Однією з величезних інформаційних атак на Інтернет за усю його історію стала атака сітьового «черв'яка» Хелкерн, яка розпочалася 26 січня 2003 року й тривала два дні. Вплив Хелкерна на світові інформаційні ресурси був визнаний експертами комп'ютерної безпеки безпрецедентним випадком за швидкістю розповсюдження та розмірам спричиненої і потенційної шкоди – більш 10 млрд. доларів. У результаті було інфіковано 80 тисяч веб-серверів, а Інтернет уповільнив свою роботу у всьому світі у середньому на 25 %. Аналітики вважають, що Хелкерн став «важливим кроком у створенні інформаційної зброї», оскільки до нього жодному вірусу не вдавалося настільки ефективно заважати обміну інтернет-трафіком.

Аналіз відомих кібератак показує, що ІКТ вже засвоєні й міжнародними терористичними й екстремістськими організаціями (Хамаз, Аль-Каїда) і національними сепаратистськими рухами. Але сьогодні терористи продовжують віддавати перевагу вбивству реальних людей справжніми бомбами, щоб налякати населення через посередництво ЗМІ, ніж заподіювати віртуальну шкоду через Інтернет. На думку експертів, проблема не стільки у кібертероризмі, скільки у кіберзлочинності та, навіть, можливої кібервійні.

Окремі зловживання засобами ІКТ призводить до превентивних заходів у боротьбі з ними. Так, наприклад, Естонія, яка постраждала від дій невідомих хакерів-злочинців, що організували у 2007 р. атаку на банківські та урядові сервери країни, скористувалася цим, щоби вступити у НАТО та заснувала два центра кібероборони: один у Брюсселі, другій – у Таллінні.

США, які створили під час «холодної війни» широку мережу телекомунікаційного шпигунства (під назвою Echelon), проголосили, що запускають план, який має забезпечити їм лідерство в кіберпросторі. Цей план став наслідком реалізації проекту «Манхеттен» (що породив першу атомну бомбу) і має на меті декілька завдань: здійснювати нагляд за світовим Інтернет-трафіком і за запитами у пошукових системах; створювати «троянські програми», що позволяють встановити контроль над будь-яким комп'ютером; і нарешті використання Інтернету (та його користувачів) для випробування сценаріїв атаки та оборони, а також для тренування військових кіберпідрозділів [1, с. 47]. Цей проект, таким чином має подвійний характер – з одного боку є одним із засобів превентивної оборони у боротьбі з кібертероризмом, а з іншої – одним із засобів реалізації геополітичних амбіцій США.

У січні 2003 р. офіційні особи США заявили про те, що Міністерство оборони може вести інформаційну війну у випадку, якщо на країну буде здійснений інформаційний напад, а на початку лютого офіційні особи з Адміністрації Президент США повідомили, що Дж. Буш підписав секретну директиву, відповідно до якої уряд вперше має розробити національне керівництво, що визначає умови, за яких Сполучені Штати будуть здійснювати кібератаки на комп'ютерні мережі своїх супротивників, а також правила проникнення в іноземні комп'ютерні системи й порушення їх нормальної роботи [2] .

Очевидно, що завдяки активному використанню ІКТ світ зіштовхнувся з новими ризиками для міжнародної безпеки, що поставили перед світовою спільнотою важливе завдання – створення міжнародно-правових заходів упередження кіберзлочинності, кібертероризму та недопущення кібервійни. Проблема світової протидії загрозам інформаційної безпеки посилюється тим, що до сих пір не вироблено загальноприйнятого визначення «інформаційної зброї». Відомо, що цей термін став використовуватися в американських військових колах у 1991 р., після закінчення війни у Персидській затоці.

Ускладнює питання про дефініції та обставина, що інформаційні технології більш всього виступають як технології невійськового або подвійного призначення. ІКТ, за допомогою яких можуть здійснюватися військові операції, головним чином починають застосовуватися у цивільному секторі. Характерними рисами інформаційної зброї є універсальність, радикальність застосування, доступність. Її впровадження не вимагає великих фінансових витрат, що робить інформаційну війну економічним, а тому небезпечним засобом військової боротьби, яка часто має характер мирної діяльності. Одночасно важко визначити й державу, що здійснило інформаційну атаку. Використання цієї зброї може відбуватися приховано, без проголошення війни і не вимагає видиму підготовку. Жертва може навіть не усвідомлювати, що знаходиться під інформаційним впливом [3] .

Важливо нагадати й про можливі загрози правам і свободам громадян у зв'язку із застосуванням інформаційної зброї. Перш за все постраждають найголовніші завоювання демократії: право на свободу розповсюдження інформації і доступу до неї, конфіденційність інформації про приватне життя людини та інше. Разом з тим інформаційні засоби впливу на людину можуть відігравати роль психотропної зброї.

Таким чином вочевидь постає необхідність забезпечення міжнародної інформаційної безпеки міжнародно-правовими засобами. Міжнародне право тільки вступає на шлях її регулювання.

10 травня 1999 р. Генсекретар ООН виступив з докладом (A/54/213), в якому визнавалася наявність проблеми у сфері міжнародної інформаційної безпеки (далі – МІБ). Резолюція 53/70 поклала початок обговорення необхідності створення нового міжнародно-правового режиму для регулювання сфери інформаційного простору, ІКТ та методи її використання [4]. У 1999 р. в Женеві пройшов міжнародний семінар з питань міжнародної інформаційної безпеки. У семінарі прийняли участь представники більше 50 країн. Його підсумком стало підтвердження актуальності проблеми інформаційної безпеки і сучасності постановки цього питання у міжнародному плані. На 54 сесії Генеральної Асамблеї ООН був запропонований проект резолюції «Досягнення у сфері інформатизації і телекомунікації у контексті міжнародної безпеки». Важливим моментом стало те, що в ньому вперше висловлювалася занепокоєність можливістю потенційного використання засобів ІКТ «з цілями, що несумісні із завданнями забезпечення міжнародної стабільності та безпеки», що може негативно вплинути на безпеку держав як у громадянській, так і у військової сферах. Вважаючи за необхідне упередити «неправомірне використання або використання інформаційних ресурсів або технологій у злочинних або терористичних цілях», ГА поставила питання про «доцільність розробки міжнародних принципів, направлених на зміцнення безпеки глобальних інформаційних і телекомунікаційних систем і сприяли боротьбі з інформаційним тероризмом і криміналом» [5]. Російською стороною був підготовлений проект "Принципів, що стосуються міжнародної інформаційної безпеки", який був опублікований в документі 55 Генеральної Асамблеї ООН A/55/140 як вклад Росії в подальше обговорення теми. В ньому знаходиться необхідна понятійна база і приводяться основні визначення: міжнародної інформаційної безпеки, погроз інформаційної безпеки, інформаційної зброї, інформаційної війни, міжнародного інформаційного тероризму і злочинності. П'ять базових принципів міжнародної інформаційної безпеки визначають роль і права, зобов'язання і відповідальність держав в інформаційному просторі.

У резолюції, прийнятій консенсусом 29 листопада 2001 року (документ A/RES/56/19), схвалена ідея створення в 2004 році спеціальної Групи урядових експертів держав-членів ООН (ГПЭ) для проведення усебічного дослідження проблеми МІБ [8]. Мандатом Групи передбачається розгляд існуючих і потенційних погроз у сфері інформаційної безпеки і можливих спільних заходів по їх усуненню, а також вивчення міжнародних концепцій, які були б спрямовані на зміцнення безпеки глобальних інформаційних і телекомунікаційних систем. Результатом роботи Групи, відповідно до резолюції, стане доповідь Генсекретаря ООН Генеральній Асамблеї в 2005 році про результати цього дослідження.

У наступний період здійснюється реалізація рішення міжнародного співтовариства про необхідність широкого практичного вивчення питань МІБ, приймаються резолюції, що розвивають положення попередніх резолюцій і підтверджують недопустимість використання інформаційно-телекомунікаційних технологій і засобів в цілях негативного впливу на інфраструктуру держав. 23 січня 2002 р. 56 ГА ООН приймає резолюцію за докладом на тему «Боротьба зі злочинним використанням інформаційної технології», де говорилося про необхідність міжнародної співпраці, а також між державами й приватними сектором у боротьбі зі злочинним використанням ІКТ, а також про необхідність сприяння надання ІКТ країнам, що розвиваються, оскільки невідповідності різних держав у рівні доступу до ІКТ та їх використанні можуть знизити ефективність боротьби зі злочинністю у цієї сфері [6]. У 2002 р. на Загальноєвропейської конференції в Бухаресті була прийнята декларація, що закріпила принцип зміцнення довіри та безпеки у процесі використання ІКТ. Вона передбачає розробку «глобальної культури кібербезпеки», що мала забезпечуватися шляхом прийняття превентивних засобів та підтримуватися усією спільнотою за умови збереження свободи передання інформації. Країни погодилися з тим, що необхідно «упереджувати використання інформаційних ресурсів або технологій зі злочинними або терористичними цілями» та зміцнювати міжнародну співпрацю у цієї сфері [8] .

У Токійській декларації (13-15 січня 2003 року), яку прийняли представники 47 країн, 22 міжнародних і 116 неурядових організацій, а також представники 54 приватних компаній, виділені "пріоритетні області дій" в області ІКТ. Важливе місце в їх числі займає питання забезпечення безпеки інформаційних технологій і засобів. Визнаючи принцип справедливого, рівного і адекватного доступу до

ІКТ для усіх країн особливу увагу сторони вважають необхідним приділити загрозі потенційного військового використання ІКТ. Уперше було висловлено думку про те, що ефективне забезпечення інформаційної безпеки може бути досягнуте не лише технологічно, для цього буде потрібно зусилля із правового регулювання питання і вироблення відповідних національних політик [2].

Нарешті, за рішеннями резолюцій ГА ООН 56/183 від 21 грудня 2001 року и 57/238 від 20 грудня 2002 року в Женеві 10-12 грудня 2003 року пройшов перший етап Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства (її другий етап був запланований на 16-18 листопада 2005 року у Тунісі). Зустріч виявилася першим міжнародним форумом, на якому обговорення питань, пов'язаних з глобальними процесами інформатизації, було підняте на самий вищий політичний рівень і відбулося в широкому геополітичному масштабі в діалозі з представниками ділових кіл і громадянського суспільства. У саміті брало участь понад 11 тисяч осіб з 176 країн світу, включаючи представників міжнародних організацій. В ході зустрічі питання інформаційної безпеки знаходилося в центрі міжнародної уваги.

Підсумком першого етапу Зустрічі стало прийняття двох документів - Декларації принципів і Плану дій. Вони охоплюють різні аспекти формування глобального інформаційного суспільства і базові напрями міждержавної взаємодії в цій сфері включаючи створення і розвиток інформаційно-комунікаційної інфраструктури, безпеку при використанні ІКТ, забезпечення доступу до інформації, інфраструктури і послуг на базі ІКТ [8] . У Декларації принципів (розділ "Зміцнення довіри і безпеки при використанні ИКТ") вказується на те, що зміцнення основи для довіри, включаючи інформаційну безпеку і безпеку мереж, є передумовою становлення інформаційного суспільства.

Важливі аспекти боротьби із інформаційною злочинністю були зафіксовані у резолюції 58 ГА ООН від 30.01.2004 року про «Створення глобальної культури кібербезпеки і захист найважливіших інформаційних структур». Найсуттєвішим з них можна назвати формулювання переліку елементів для захисту найважливіших інформаційних інфраструктур. Тобто були вказані ті захисні механізми, як міжнародного так і національного рівня, котрі є базовими елементами для побудови глобальної системи протидії спробам використання і використанню ІКТ у цілях не сумісними з основними принципами міжнародного права та безпекою держав, суспільства та особи.

Аналізуючи законодавство України з питань, що стосуються інформаційної безпеки, можна зробити висновок про визнання державою проблем пов'язаних з інформаційною безпекою.

Певною мірою визнання існування проблем пов'язаних з інформаційною безпекою є прийняття юридичних норм, що регулюють суспільні відносини у даній сфері. Наприклад:

- Закон України "Про захист інформації в інформаційно-телекомунікаційних системах",
- Закон України "Про державну таємницю",
- Закон України "Про основи національної безпеки України",
- Указ Президента України № 891 від 24.09.2001 року "Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних",
- Указ Президента України № 1229 від 27.09.1999 року "Про Положення про технічний захист інформації в Україні" тощо.

Знов-таки, певною мірою визнання того факту, що у даній сфері суспільних відносин можуть траплятися кримінальні прояви є прийняття нормативних документів, котрі встановлюють відповідальність за злочини скоєні в інформаційній сфері. Прикладом можуть бути:

- Розділ 16 Кримінального Кодексу України «Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж»,
- визначення «технологічного тероризму» у Законі України «Про боротьбу з тероризмом», де говориться про злочини, що вчиняються з терористичною метою із застосуванням засобів електромагнітної дії, комп’ютерних систем та телекомунікаційних мереж.

Але хотілось більш детально звернути увагу на положення Указу Президента України «Про Доктрину інформаційної безпеки України» № 514/2009 від 08.07.2009 р., які визначають позицію нашої держави, саме у сфері міжнародній інформаційній безпеці. Так напрямами діяльності у сфері зовнішньої політики, зокрема, є:

- якісне вдосконалення інформаційного супроводу державної політики, діяльності українських громадських організацій та суб'єктів підприємницької діяльності за кордоном за пріоритетами стратегічного партнерства та економічної доцільності;

- організаційно-технічне, інформаційне та ресурсне сприяння держави вітчизняним засобам масової інформації, які мають формувати у світовому інформаційному просторі позитивний імідж України;

- посилення інформаційно-просвітницької діяльності серед населення щодо забезпечення національної безпеки України за умов повноправного партнерства з країнами - членами ЄС та Північноатлантичного альянсу;

- інтеграція в міжнародні інформаційно-телекомунікаційні структури та організації на засадах рівноправності, економічної доцільності та збереження інформаційного суверенітету;

- гарантування своєчасного виявлення зовнішніх загроз національному інформаційному суверенітету та їх нейтралізації [9].

Висновки.

У підсумку зазначимо, що латентність розробки засобів ведення інформаційних воєн; належність ІКТ до технологій подвійного призначення, та поєднання цих технологій з традиційними засобами ведення бойових дій при, практично, безконтрольному створенні, використанні і слабкому регулюванні кіберпростору може привести до катастрофічних наслідків для існування людської цивілізації. Запобігти цьому може тільки міжнародна співпраця всіх держав у сфері міжнародної інформаційної безпеки, яка на основі збалансованих міжнародних нормативно-правових актів з урахуванням специфіки національних законодавств та наявності політичної волі держав зможе забезпечити створення ефективної системи міжнародної інформаційної безпеки.

ДЖЕРЕЛА І ЛІТЕРАТУРА

1. Иноземцев В.Л., Кузнецова Е.С. Атлас 2010. Le monde diplomatique / Иноземцев В.Л. – М.: Центр исследования постиндустриального общества, 2010. – 224 с.
2. Крутских А. К политико-правовым основаниям глобальной информационной безопасности. – Режим доступу : // www.portalus.ru/modules/internationallaw/ rus_readme.php?
3. А.В. Крутских, И.Л. Сафонова. Международное сотрудничество в области информационной безопасности – Режим доступу :// www.ict.edu.ruft002472intcoop.pdf).pdf
4. Борьба с преступным использованием информационных технологий: Резолюция Генеральной Ассамблеи ООН 53/70 от 4 января 1999. – С. 1–2. – Режим доступу ://www.un.org/russian/documen/gadocs/53sess/53reslis.htm
5. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности: Резолюция Генеральной Ассамблеи ООН 54/49 от 23 сентября 1999. – С. 1–2. – Режим доступу: http://www.un.org/russian/documen/gadocs/54sess/54reslis.htm
6. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности: Резолюция Генеральной Ассамблеи ООН 56/121 от 23 января 2002. – С. 1–2. – Режим доступу: //www.un.org/russian/documen/gadocs/56sess/56reslis.htm
7. Создание глобальной культуры кибербезопасности: Резолюция Ассамблеи ООН 57/239 от 31 января 2003. – С. 1–3. – Режим доступу : //www.un.org/russian/documen/gadocs/57sess/57reslis.htm
8. Международное сотрудничество в области информационной безопасности (справочная информация). – Режим доступу: //www.ln.mid.ru/ns-dvbr.nsf/0/4c86fcb9f8dc1b41c3256e320029b1ef?OpenDocument
9. Указ Президента України «Про Доктрину інформаційної безпеки України» від 08.07.2009 р., № 514/2009 // Офіційний вісник України. – 2009. – №52. – Ст. 1783.

Широкова-Мурараш О. Г., Акчурин Ю. Р. Международно-правовые мероприятия относительно упреждения преступности в сфере информационной безопасности / Институт международных отношений Национального авиационного университета.

В статье исследуется проблема международно-правового предупреждения киберпреступности и кибертерроризма как результата негативного влияния информационных технологий на общество.

Ключевые слова: *информационные телекоммуникационные технологии, кибертерроризм, киберпреступность, информационная безопасность, информационная война, резолюции ООН*

O. Shyrokova-Murarash, Y. Akchurin. International law measures in relation to prevention of criminality in the field of informative safety / Institute of International Relations National Aviation University.

The article researches the problem of international law prevention of the cyberterrorism and cybercrime as a result of the negative influence of information technology on society.

Key words: *information telecommunication technologies, cyberterrorism, cybercrime, informative safety, informative war, resolutions of UNO.*