УДК:004.056: 341(045)

**ШИРОКОВА-МУРАРАШ О.Г.,** доцент кафедри міжнародного права
Інституту міжнародних відносин
Національного авіаційного університету
**АКЧУРІН Ю.Р.,** старший викладач кафедри міжнародного права
Інституту міжнародних відносин
Національного авіаційного університету

# КІБЕРЗЛОЧИННІСТЬ ТА КІБЕРТЕРОРИЗМ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ: МІЖНАРОДНО-ПРАВОВИЙ АСПЕКТ

***Анотація.*** *До проблеми міжнародно-правового упередження кіберзлочинності та кібертероризму як результату негативного впливу інформаційних технологій на суспільство.*

***Аннотация.*** *К проблеме международно-правового предупреждения киберзлочинности и кибертерроризма как результата негативного влияния информационных технологий на общество.*

***Summary.*** *As to the problem of international law prevention of cyber crime and cyber terrorism as a result of the negative impact of information technologies on the society.*

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

Сучасний світ неможливо 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. ІКТ стали одним з основних факторів забезпечення та підтримки стабільного розвитку, а кількість, технічний рівень та доступність інформаційних ресурсів визначають рівень розвитку країни та її статус у світовому співтоваристві. У той же час розвиток ІКТ обумовив не лише перехід національних інфраструктур на принципово новий рівень розвитку та функціонування, а й призвів до виникнення принципово нових загроз системам національної та міжнародної безпеки і породив цілий комплекс негативних геополітичних наслідків. Ці загрози пов’язані насамперед з можливістю використання ІКТ у цілях, несумісних з підтримкою 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 в 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 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 у 1993 році футурологом Елвіном Тоффлером, коли широка публіка ще мало що знала про Інтернет. Тоффлер 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 сьогодні у світі не було зареєстровано жодного кібертерористичного акту. Такого висновку дійшов у своїй доповіді “Кибертероризм: 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 поширення своєї пропаганди на веб-сайтах, форумах і у формі відеороликів, передусім 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 результатом зусиль любителів чи груп фанатиків, і поки що вони не спричинили великих матеріальних або фінансових, а тим більше людських, втрат.

Однією з величезних інформаційних атак на Інтернет за всю його історію стала атака мержного “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 – понад 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 віртуальної шкоди через Інтернет. На думку експертів, проблема не стільки у кібертероризмі, скільки у кіберзлочинності, навіть, у можливості початку кібервійни.

Окремі зловживання засобами ІКТ призводять до превентивних заходів у боротьбі з ними. Наприклад, Естонія, яка постраждала від хакерів-злочинців, що організували у 2007 р. атаку на банківські та урядові сервери країни, скористалася цим, щоб вступити у НАТО, та заснувала два центри кібероборони: один у Брюсселі, другий – 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 дозволяють 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]. Таким чином, цей проект має подвійний характер – з одного боку, є одним із засобів превентивної оборони у боротьбі з кібертероризмом, а з іншого – 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 Президента 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 сьогодні не вироблено загальноприйнятого визначення терміна “інформаційна зброя”. Цей термін став використовуватися в американських військових колах у 1991 р., після закінчення війни у Перській затоці.

Ускладнює питання про дефініції та обставина, що інформаційні технології здебільшого 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 здійснила інформаційну атаку. Використання цієї зброї може відбуватися приховано, без оголошення війни, і не вимагає видимої підготовки. 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. Насамперед постраждають найголовніші завоювання демократії: право на свободу поширення інформації і доступу до неї, конфіденційність інформації про приватне життя людини та ін. Разом з тим, інформаційні засоби впливу на людину можуть відігравати роль психотропної зброї. Вочевидь постає необхідність забезпечення міжнародної інформаційної безпеки міжнародно-правовими засобами.

Міжнародне право тільки вступає на шлях її регулювання. 10 травня 1999 року Генсекретар ООН виступив з доповіддю (A/54/213), в якій визнавалася наявність проблеми у сфері міжнародної інформаційної безпеки (далі – МІБ). Резолюція № 53/70 поклала початок обговоренню необхідності створення нового міжнародно-правового режиму для регулювання сфери інформаційного простору, ІКТ та методів її використання [4]. У 1999 році в Женеві пройшов міжнародний семінар з питань міжнародної інформаційної безпеки. У його роботі взяли участь представники більш як 50 країн. Підсумком стало підтвердження актуальності проблеми інформаційної безпеки і сучасності постановки цього питання у міжнародному плані. На 54-ій 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 цивільній, так і у

військовій сферах. Вважаючи за необхідне упередити “неправомірне використання або використання інформаційних ресурсів чи технологій у злочинних або терористичних цілях”, Генеральна Асамблея поставила питання про “доцільність розробки міжнародних принципів, направлених на зміцнення безпеки глобальних інформаційних і телекомунікаційних систем і сприяння боротьбі з інформаційним тероризмом і криміналом” [5]. Російською стороною був підготовлений проект “Принципів, що стосуються міжнародної інформаційної безпеки”, який був опублікований в документі 55-ої Генеральної Асамблеї ООН № А/55/140 як вклад Росії в подальше обговорення теми. В ньому міститься необхідна понятійна база і наводяться основні визначення: міжнародної інформаційної безпеки, загроз 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 (ГУЄ) для проведення усебічного дослідження проблеми МІБ [8]. Мандатом Групи передбачається розгляд існуючих і потенційних загроз 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 з метою негативного впливу на інфраструктуру держав. 23 січня 2002 році. 56-та ГА ООН приймає резолюцію щодо доповіді на тему “Боротьба зі злочинним використанням інформаційної технології”, де говорилося про необхідність міжнародної співпраці, а також взаємодії між державами й приватним 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 цій сфері [6]. У 2002 році на Загальноєвропейській 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 вжиття превентивних заходів 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 цій 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” у сфері 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 за необхідне 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 потрібні зусилля із правового регулювання питання і вироблення відповідних національних політик [2].

Нарешті, згідно з рішеннями резолюцій ГА ООН № 56/183 від 21 грудня 2001 року та № 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 порушено на найвищому політичному рівні і відбулося в широкому геополітичному масштабі в діалозі з представниками ділових кіл і громадянського суспільства. У саміті брали участь понад 11 тисяч осіб з 176 країн світу, включаючи представників міжнародних організацій. В ході зустрічі питання інформбезпеки 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 ІКТ”) вказується на те, що зміцнення основи для довіри, включаючи інформаційну безпеку і безпеку мереж, є передумовою становлення інформаційного суспільства.

Важливі аспекти боротьби з інформаційною злочинністю були зафіксовані у Резолюції 58-ої ГА ООН від 30.01.2004 року “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 сумісних 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 визнанням існування проблем, пов’язаних з інформаційною безпекою, є прийняття юридичних норм, що регулюють суспільні відносини у даній сфері. Наприклад, закони України “Про захист інформації в інформаційно-телекомунікаційних системах”, “Про державну таємницю”, “Про основи національної безпеки України”, укази Президента України № 891 від 24.09.01 р. “Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних” та № 1229 від 27.09.99 р. “Про Положення про технічний захист інформації в Україні” тощо.

Знову-таки, певною мірою визнанням того факту, що в 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 вчинюються з терористичною метою із застосуванням засобів електромагнітної дії, комп’ютерних систем та телекомунікаційних мереж.

Але хотілося б більш детально звернути увагу на положення Указу Президента України “Про Доктрину інформаційної безпеки України” № 514/2009 від 08.07.09 р., які визначають позицію нашої держави саме у сфері міжнародної інформаційній безпеки. 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 призвести до катастрофічних наслідків для існування людської цивілізації. Запобігти цьому може тільки міжнародна співпраця всіх держав у сфері інформаційної безпеки, яка на основі збалансованих міжнародних нормативно-правових актів з урахуванням специфіки національних законодавств та наявності політичної волі зможе забезпечити створення ефективної системи міжнародної інформаційної безпеки.

## Використана література

1. Иноземцев В.Л., Кузнецова Е.С. Атлас 2010. Le monde diplomatique / В.Л. Иноземцев. – М. : Центр исследования постиндустриального общества, 2010. – 224 с.

2. – 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 04.01.99 г. – 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 23.09.99 г. – С. 1-2. – Режим доступу : //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 23.01.02 г. – С. 1-2. – Режим доступу: //www.un.org/russian/documen/gadocs/56sess/56reslis.htm

7. Создание глобальной культуры кибербезопасности: Резолюция Генеральной Ассамблеи ООН № 57/239 от 31.01.03 г. – С. 1-3. – Режим доступу : //www.un.org/russian/documen/gadocs/57 sess/57reslis.htm

8. Международное сотрудничество в области информационной безопасности (справочная информация). – Режим доступу : //www.ln.mid.ru/ns-dvbr.nsf/0/4c86fcb9f8dc1b41c3256e320029b1 ef?OpenDocument

9. Про Доктрину інформаційної безпеки України : Указ Президента України від 08.07.09 р. № 514/2009 // Офіційний вісник України. – 2009. – № 52. – Ст. 1783.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~