ISSN 1995-6134

УДК 004.056(075.8)
О.В. БОЙЧЕНКО, канд. техн. наук, доц.,
Кримський юридичний інститут Одеського державного університету внутрішніх справ

МІЖНАРОДНА ІНФОРМАЦІЙНА БЕЗПЕКА: ПРОБЛЕМИ І ПЕРСПЕКТИВИ

Ключові слова: *інформаційно-комунікаційні технології, Декларація принципів міжнародної інформаційної безпеки, Доктрина інформаційної безпеки*

Стрімкий розвиток інформаційно-комунікаційних технологій (ІКТ) сприяє налагодженню широкої міжнародної співпраці. Проте окремі досягнення в інформаційній сфері можуть бути використані в цілях, що суперечать підтримці міжнародної безпеки та стратегічної стабільності. Ростуть масштаби кіберзлочинності та кібертероризму [1]. Особливу заклопотаність викликає можливість застосування інформаційно-телекомунікаційних технологій для підготовки та здійснення терористичних актів у світі.

Дослідженню проблем міжнародної інформаційної безпеки (МІБ) стосовно сучасних концепцій міжнародної безпеки, міжнародної безпеки через співробітництво, інформаційної безпеки в масово-комунікаційній сфері приділялася увага в роботах таких видатних фахівців, як С.П. Расторгуєв, О.Г. Білорус, Д.Г. Лук'яненко, Є.А. Макаренко, А.М. Гуз та інших [2-4].

Комплексні дослідження проблем і перспектив становлення ефективного механізму заходів МІБ у колі питань міжнародних відносин держав до нашого часу не проводились. Поряд із зазначеним необхідність подальшого наукового дослідження проблем та перспектив МІБ обґрунтовує також висока динаміка розвитку міжнародних відносин при стрімкому розвитку інформаційно-телекомунікаційних систем і технологій.

Зазначене свідчить про те, що дослідження проблем і перспектив МІБ у напрямку нормативно-правового регулювання питань захисту інформаційних ресурсів, які формуються та постійно циркулюють у складі інформаційно-телекомунікаційних систем під час здійснення міжнародних відносин державами, має відповідну наукову новизну. Метою роботи є комплексне вивчення проблем, пов'язаних з питаннями МІБ, а також розробка пропозицій щодо розвитку системи заходів міжнародної інформаційної безпеки, основою якої є відповідні міжнародні нормативно-правові акти.

Як уже зазначалося, стрімкий розвиток і широке використання ІКТ привів до формування фундаментальної залежності критичних національних інфраструктур від цих технологій і зумовив виникнення принципово нових загроз. Ці загрози пов'язані, насамперед, з можливістю використання ІКТ в цілях, несумісних із завданнями підтримки міжнародної стабільності та безпеки, дотримання принципів відмови від застосування сили, невтручання у внутрішні справи держав, забезпечення прав і свобод людини.

Загострення потенційної небезпеки обґрунтована можливістю розробки, застосування та розповсюдження інформаційної зброї, загрозою інформаційних війн і інформаційного тероризму, здатних викликати інформаційні конфлікти зі значними руйнівними наслідками.

Тому силами міжнародних співтовариств організується та впроваджується в життя комплекс необхідних заходів МІБ, основою якого є міжнародні Договори та Декларації за результатами самітів держав та резолюції Генеральних Асамблей (ГА) ООН.

Так, ще в 1998 році за результатами 53-ої сесії ГА ООН розроблено резолюцію (A/RES/53/70) «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки», яка пропонує державам-членам ООН продовжити обговорення питань інформаційної безпеки, дати конкретні визначення погроз, запропонувати свої оцінки проблеми, включаючи розробку міжнародних принципів забезпечення безпеки глоба-

ISSN 1995-6134

льних інформаційних систем.

Резолюція 53/70 поклала початок обговоренню створення абсолютно нового міжнародно-правового режиму, суб'єктом якого в перспективі повинні стати інформація та інформаційна технологія.

Відповідно до її рекомендацій, Інститутом ООН з проблем роззброєння та Департаментом з питань роззброєння Секретаріату ООН в серпні 1999 року в Женеві був організований міжнародний семінар з питань МІБ, у роботі якого прийняли участь представники більше 50 країн найбільш розвинених в інформаційно-технологічному плані.

Завдання семінару полягало у виявленні підходів різних країн у зв'язку з майбутнім продовженням дискусії з проблем МІБ на 54-ій сесії ГА ООН. Основним підсумком семінару стало підтвердження актуальності проблеми інформаційної безпеки і своєчасності постановки цього питання на міжнародному рівні.

У 1999 році на 54-ій сесії ГА ООН було прийнято оновлений проект резолюції (A/RES/54/49) «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки», який вперше вказав на погрози МІБ відносно не тільки до цивільної, але і до військової сфер. Поряд із зазначеним, за результатами роботи сесії було опубліковано проект «Принципів, що стосуються міжнародної інформаційної безпеки» (A/55/140У).

Принципи є свого роду робочим варіантом кодексу поведінки держав в інформаційному просторі, створюючи для них відповідні моральні зобов'язання, а також закладають основу для широких міжнародних переговорів під егідою ООН і інших міжнародних організацій з проблем МІБ. У них міститься необхідна понятійна база з предмету МІБ, наводяться основні визначення: міжнародної інформаційної безпеки, погроз інформаційній безпеці, інформаційної зброї, інформаційної війни, міжнародного інформаційного тероризму та злочинності.

П'ять базових принципів МІБ визначають роль і права, зобов'язання та відповідальність держав в інформаційному просторі, намічають конкретні завдання, вирішення яких було б направлене на обмеження погроз у сфері МІБ, а також прописують роль ООН в контексті загальних зусиль в цій сфері.

За результатами роботи 55-ій сесії ГА ООН у 2000 році схвалено новий проект резолюції (A/RES/55/28), в якому наголошується, що цілям обмеження погроз у сфері інформаційної безпеки відповідало би «вивчення відповідних міжнародних концепцій, направлених на зміцнення безпеки глобальних інформаційних і телекомунікаційних систем». Дане положення було надзвичайне важливим з дипломатичної і політичної точок зору, оскільки стало підґрунтям для наступного дуже важливого етапу вирішення проблем МІБ в ООН.

Крім того, відповідно до рекомендацій резолюції 55/28, було підготовлено проект документу (A/56/164/Add.1) «Загальна оцінка проблем інформаційної безпеки. Погрози міжнародній інформаційній безпеці», в якому виділені та описані одинадцять основних чинників, що створюють небезпеку основним інтересам особи, суспільства і держави в інформаційному просторі, тобто є найбільшими загрозами МІБ.

До таких чинників відносяться:

- розробка і використання засобів несанкціонованого втручання в роботу ІКТ, неправомірне використання та нанесення збитку інформаційним ресурсам іншої держави;
- цілеспрямована інформаційна дія на критичні інфраструктури і населення іншої держави;
- дії, направлені на домінування в інформаційному просторі, заохочення тероризму та ведення інформаційних війн.

У резолюції A/RES/56/19, яка була прийнята у 2001 році схвалена ідея створення в 2004 році спеціальної Групи урядових експертів держав-членів ООН (ГУЕ) для проведення усестороннього дослідження проблеми МІБ.

Прерогативою діяльності ГУЕ повинен стати розгляд існуючих і потенційних погроз у сфері інформаційної безпеки та сумісних

ISSN 1995-6134

заходів з їх усунення, а також вивчення міжнародних концепцій зміцнення безпеки глобальних інформаційних і телекомунікаційних систем.

Прийнята консенсусом 22.11.2002 року ГА ООН резолюція по МІБ (A/RES/57/53) розвиває положення попередніх резолюцій і вказує на неприпустимість використання інформаційно-телекомунікаційних технологій і засобів в цілях надання негативної дії на інфраструктуру держав. Резолюція визначає також напрями діяльності ГУЕ ООН, робота якої повинна концентруватися на наступних ключових моментах:

- узгодження понятійного апарату у сфері МІБ;
- розгляд чинників, що впливають на стан МІБ з урахуванням наявності загроз терористичного, кримінального та військового характеру;
- визначення взаємоприйнятних заходів запобігання використанню інформаційних технологій та засобів в терористичних і інших злочинних цілях, а також заходів щодо обмеження застосування інформаційної зброї, перш за все відносно критично важливих структур держав;
- розгляд можливих шляхів міжнародної взаємодії правоохоронних органів по запобіганню і припиненню правопорушень в інформаційному просторі, зокрема, по виявленню джерел інформаційної агресії;
- аналіз проблеми регулювання національних законодавств окремих країн щодо питань інформаційної безпеки для забезпечення уніфікованої класифікації правопорушень у сфері інформаційної безпеки, а також визначення відповідальності, яка виникає у зв'язку зі здійсненням дій, що класифікуються як злочинні;
- оцінка можливості надання міжнародної допомоги країнам, що стали жертвами інформаційних атак, в цілях пом'якшення наслідків порушення нормальної діяльності перш за все об'єктів критичних інфраструктур держав.

Основною ідеєю створення універсального режиму МІБ могло би стати зобов'язання учасників не вдаватися до дій в інформаційному просторі, метою яких є нанесення збитку інформаційним мережам, системам, ресурсам, процесам та інфраструктурі іншої держави, підрив політичної, економічної та соціальної систем, масована психологічна обробка населення, задля дестабілізації суспільства і держави.

За результатами роботи ГА ООН в Женеві, Тунісі, Бухаресті, Токіо та інших країнах учасники дійшли до розуміння того, що «ІКТ можуть використовуватися в цілях, несумісних із завданнями забезпечення міжнародної стабільності та безпеки, а також негативно впливати на цілісність інфраструктури усередині окремих держав, порушуючи їх безпеку як в цивільній, так і у військовій сфері». Країни також погодилися з тим, що необхідно «запобігати використанню інформаційних ресурсів або технологій в злочинних або терористичних цілях». У основу цих положень лягла консенсусна резолюція ГА ООН по МІБ № 56/19.

Зокрема, в резолюції зафіксовано, що в цілях сприяння довірі та безпеки у використанні ІКТ, органи державного управління повинні сприяти усвідомленню суспільством погроз, пов'язаних з кібербзлочинністю, і прагнути укріплювати міжнародну співпрацю в цій сфері.

Крім того, слід зазначити, що важливе місце в рішеннях резолюції займає питання забезпечення безпеки інформаційних технологій і засобів. Визнаючи принцип справедливого, рівного і адекватного доступу до ІКТ для всіх країн, особлива увага приділяється загрозі потенційного військового використання ІКТ, посиленню регіональної та міжнародної співпраці з метою зміцнення безпеки інфосфери. Вперше було висловлено думку про те, що ефективне забезпечення інформаційної безпеки може бути досягнуте не тільки технологічно, але й за рахунок правового регулювання питань МІБ і проведення відповідних національних політик.

Щодо основних результатів співпраці міжнародного співтовариства, то основними

ISSN 1995-6134

підсумковими документами за результатами міжнародних форумів з МІБ на вищому рівні стало ухвалення двох основних документів – Декларації принципів і Плану дій, які охоплюють різні аспекти формування глобального інформаційного суспільства та базові напрями міждержавної взаємодії в цій сфері, включаючи створення та розвиток інформаційно-комунікаційної інфраструктури, безпеку при використанні ІКТ, забезпечення доступу до інформації, інфраструктури та послуг на базі ІКТ.

Так, у Декларації принципів (розділ «Зміцнення довіри і безпеки при використанні ІКТ») указується на те, що зміцнення основи для довіри, включаючи інформаційну безпеку та безпеку мереж, є передумовою становлення інформаційного суспільства.

У Декларації також зафіксовано, що держави, що прийняли її, визнаючи принципи універсального і недискримінаційного доступу до ІКТ для всіх країн, підтримують діяльність ООН, направлену на запобігання можливості використання ІКТ в цілях, які несумісні із завданнями забезпечення міжнародної стабільності та безпеки, а також таких, які здатні надати негативну дію на цілісність державних інфраструктур, завдаючи збитку їх безпеці. Вони також виходять з того, що слід запобігати використанню інформаційних ресурсів і технологій в злочинних і терористичних цілях.

Слід також зазначити, що одним із принципів інформаційного суспільства став принцип зміцнення довіри і безпеки при використанні ІКТ, що визначає розробку «глобальної культури кібербезпеки», яка повинна забезпечуватися шляхом застосування превентивних заходів і підтримуватися всім суспільством при збереженні свободи передачі інформації. У Плані дій наголошується, що довіра й безпека відносяться до головних засад інформаційного суспільства.

Поряд із цим виділені найважливіші напрями дій із зміцнення довіри і безпеки при використанні ІКТ, зокрема:

- сприяння співпраці між державами в рамках ООН і зі всіма зацікавленими сторонами в рамках відповідних форумів з метою аналізу існуючих і потенційних загроз у сфері ІКТ, а також вирішення інших питань інформаційної безпеки та безпеки мереж;

- попередження та виявлення органами державного управління в співпраці з приватним сектором проявів кіберзлочинності та неналежного використання ІКТ, а також реагування на ці прояви шляхом розробки відповідних керівних принципів;

- вивчення законодавства, яке дає можливість ефективно розслідувати і піддавати переслідуванню неналежне використання ІКТ;

- сприяння ефективним заходам взаємодопомоги в цій сфері, а також профілактиці комп'ютерних інцидентів;

- обмін зразками якнайкращої практики в сфері інформаційної безпеки і безпеки мереж, заохочення їх використання всіма зацікавленими сторонами;

- призначення координаторів у всіх зацікавлених країнах для реагування в режимі реального часу на події у сфері безпеки та формування відкритої сумісної мережі таких координаторів для обміну інформацією та технологіями реагування на події;

- заохочення активної участі зацікавлених країн в ООН діяльності по зміцненню довіри та надійності при використанні ІКТ [5].

Аналіз проведених державами заходів на міжнародному рівні визначає доволі великий обсяг робіт, що спрямовані на створення дієвого механізму системи заходів міжнародної інформаційної безпеки. Але сьогодення свідчить про наявність глобальних проблем міжнародної інформаційної безпеки, які визначаються наперед за все зростанням міжнародної кіберзлочинності, комп'ютерного тероризму та інформаційними війнами.

Крім того, на нашу думку, одним із специфічних проявів проблематики МІБ є те, що інформаційні війни, які зараз відбуваються, не тільки підсилюють найрозвиненіші країни, але й дають шанс стати на один рівень із ними країнам колишнього другого і третього світу. Це пов'язано з асиметричним характе-

ISSN 1995-6134

ром інформаційної зброї.

Така її властивість дозволяє будь-якій державі в критичний момент вести боротьбу з сильнішим противником. Застосування інформаційної зброї в цьому випадку виявляється найбільш адекватною відповіддю на сторонні агресивні дії.

Істотні прояви інформаційних чинників міжнародної безпеки кардинально змінили оцінку 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. Аналіз показує, що позиція розвинутих країн визначається пильною увагою до інформації, яка по праву вважається одним з головних факторів володіння сучасним світом, а саме:

- визнання проблеми міжнародної інформаційної безпеки як гіпотетичного силового протистояння;
- перенесення розгляду 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. Декілька іншою є позиція країн, які не належать до західної моделі цивілізації.

Зокрема, така позиція визначається наступними напрямами:

- надання пропозицій щодо 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;
- спільні розробки технології глобального захисту від інформаційної агресії.

Аналізуючи законодавство України з інформаційної безпеки, слід зазначити ряд положень Указу Президента України «Про Доктрину інформаційної безпеки України» № 514/2009 від 08.07.2009 р., які визначають позицію нашої держави щодо перспектив міжнародній інформаційній безпеці. Так, зокрема, напрямами діяльності у зовнішньополітичній сфері 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 [6].

Підсумовуючи зазначимо, що враховуючи високу здатність інформаційних озброєнь до інтеграції з іншими традиційними і технологічно новими видами військових засобів, потенційні наслідки безконтрольного застосування багатошарового інформаційного простору можуть виявитися катастрофічними для існування людства.

Таким чином, тільки широке багатостороннє співробітництво держав у сфері міжнародної інформаційної безпеки може гарантувати світові вирішення нових складних проблем інформаційної доби і забезпечити реальну міжнародну інформаційну безпеку через впровадження комплексу заходів інформаційної безпеки на основі виважених міжнаро-

ISSN 1995-6134

дних нормативно-правових актів з урахуванням специфіки національних законодавств.

ЛІТЕРАТУРА

1. Бойченко О. В. Міжнародне співробітництво правоохоронних органів держав в галузі забезпечення інформаційної безпеки / О. В. Бойченко // Форум права. – 2009. – № 2. – С. 56–62 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2009-2/09bovzou.pdf.

2. Макаренко Є. А. Політичні доктрини глобальної інформаційної безпеки / Є. А. Макаренко // Вісник Ін-ту міжнародних відносин Київськ. нац. ун-ту імені Тараса Шевченка. – 2007. – № 2. – С. 45-51.

3. Гуз А. М. Історія захисту інформації в Україні в Україні та провідних країнах світу : навчальний посібник [для студ. вищ. навч. закл.] / А. М. Гуз. – К. : КНТ, 2007. – 260 с.

4. Білорус О. Г. Глобалізація і безпека розвитку : монографія / О. Г. Білорус, Д. Г. Лук'яненко. – К. : КНЕУ, 2001. – 733 с.

5. Підсумкові документи Всесвітнього самміту з питань інформаційного суспільства / Міністерство транспорту та зв'язку України, Державний Департамент з питань зв'язку та інформатизації. – К., 2006. – 77 с.

6. Указ Президента України «Про Доктрину інформаційної безпеки України» : від 08.07.2009 р., № 514/2009 // Офіційний вісник України. – 2009. – №5 2. – Ст. 1783.

Бойченко О. В. Міжнародна інформаційна безпека: проблеми і перспективи / О. В. Бойченко // Форум права. – 2009. – № 3. – С. 74–79 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2009-3/09bovpip.pdf

Проведено аналіз сучасних проблем міжнародної інформаційної безпеки. Визначено, що загострення потенційної небезпеки обґрунтовано можливістю розробки, застосування та розповсюдження інформаційної зброї, загрозою інформаційних війн і інформаційного тероризму. Запропоновано вирішення проблем міжнародної інформаційної безпеки через впровадження комплексу заходів інформаційної безпеки на основі визнаних міжнародних нормативно-правових актів з урахуванням специфіки національних законодавств.

***

Бойченко О. В. Международная информационная безопасность: проблемы и перспективы

Проведен анализ современных проблем международной информационной безопасности. Установлено, что обострение потенциальной опасности обосновано возможностью разработки, применения и распространения информационного оружия, угрозой информационных войн и информационного терроризма. Предложено решение проблем международной информационной безопасности посредством внедрения комплекса мер информационной безопасности на основе обоснованных международных нормативно правовых актов с учетом специфики национального законодательства.

***

Boychenko O.V. International Informative Safety: Problems and Prospects

The analysis of modern problems of international informative safety is conducted. It is set that intensifying of potential danger is grounded possibility of development, application and distribution of informative weapon, threat of informative wars and informative terrorism. Solution of problems of international informative safety is offered by means of introduction of complex of informative safety measures on the basis of grounded international normatively legal acts taking into account the specific of national legislation.