УДК 342.5:002.6

НАСТЮК В.Я., *доктор юридичних наук, професор,*
член-кореспондент НАПрН України,
БЄЛЄВЦЕВА В.В., *кандидат юридичних наук, старший науковий співробітник*

ПРАВОВІ ЗАСАДИ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА ЩОДО ПРОТИДІЇ ІНФОРМАЦІЙНИМ ПРАВОПОРУШЕННЯМ

Анотація. *Про правові аспекти міжнародного співробітництва з протидії інформаційним правопорушенням. У роботі наведені підходи до визначення поняття “інформаційна безпека”, причини та умови порушення інформаційного правопорядку у світовому просторі. Автори статті у висновках висвітлили основні засади та напрями міжнародної співпраці щодо протидії інформаційним правопорушенням.*

Ключові слова: *інформаційні правопорушення; інформаційний правопорядок; інформаційна безпека.*

Аннотация. *О правовых аспектах международного сотрудничества относительно противодействия информационным правонарушением. В работе приведены подходы к определению понятия “информационная безопасность”, причины и условия нарушения информационного правопорядка в мировом пространстве. Авторы статьи в выводах осветили основные принципы и направления международного сотрудничества по вопросам противодействия информационным правонарушениям.*

Ключевые слова: *информационные правонарушения; информационный правопорядок; информационная безопасность.*

Summary. *About the legal aspects of international cooperation in relation to counteraction by informative offence. This work presents approaches to determination of “information safety” concept, causes and conditions of offence of information law and order in international space. The authors of the article proposed in conclusions basic concepts and ways to counteraction information offence.*

Keywords: *information offences; information law order; information safety.*

Постановка проблеми. Забезпечення національної безпеки України, безпеки її національних інтересів в інформаційній сфері в сучасних умовах припускає пріоритетний розвиток системи правового регулювання правовідносин у сфері протидії викликам і загрозам цим інтересам і впорядкування відповідного правотворчого процесу. Це обумовлено, по-перше, тим, що в умовах побудови правової держави і громадянського суспільства діяльність органів державної влади, що несуть основну відповідальність за національну безпеку, повинна регулюватися певними правовими нормами, що забезпечують дотримання конституційних прав і свобод громадян.

По-друге, правотворчий процес є єдиним видом діяльності, в якому на основі встановленого Конституцією України принципу розподілу влади та предметів ведення, беруть участь усі найвищі органи державної влади. Правотворчість в інформаційній сфері спрямована на нормативне закріплення цілей протидії викликам і загрозам національній безпеці України, засобів і методів їх досягнення, забезпечення узгодженої діяльності органів влади.

По-третє, інтеграція України до міжнародного співтовариства істотно розширює можливості зміцнення інформаційної безпеки країни за рахунок участі в розвитку норм міжнародного права, створення міжнародної системи забезпечення безпеки інформаційної сфери як світу в цілому, так і кожної держави окремо.

Нарешті, по-четверте, реалізація гарантій прав і свобод громадян, захисту національних інтересів в інформаційній сфері України припускає істотне посилення ролі держави в регулюванні відповідних суспільних відносин, наявність відкритої і зрозумілої державної політики в інформаційній сфері.

На цей час дані питання знаходяться під пильною увагою науковців, серед яких слід відзначити І.В. Арістову, А.А. Баранова, І.Л. Бачилова, К.І. Бєлякова, В.М. Брижка, О.П. Дзьобаня, Р.А. Калюжного, Л.П. Коваленко, В.А. Копилова, А.І. Марущака, В.Г. Пилипчука, М.М. Рассолова, Н.А. Савінову, М.Я. Швеця та ін.

Метою статті є розгляд правових питань міжнародного співробітництва у сфері забезпечення інформаційної безпеки під кутом протидії інформаційним правопорушенням.

Виклад основного матеріалу. У доповіді Генерального Секретаря ООН від 10 серпня 1999 року “Досягнення у сфері інформатизації і телекомунікації в контексті міжнародної безпеки”, зокрема, наголошується, що збільшення за рахунок новітніх інформаційних технологій військового потенціалу країн веде до зміни глобального і регіонального балансу сил, виникнення напруженості між традиційними центрами сили і впливу. Формується принципово нова сфера протиборства на міжнародній арені, створюється ризик нового витка гонки озброєнь на основі науково-технічних досягнень у сфері інформатизації і зв’язку. При цьому зачіпається як сфера національної безпеки окремих держав, так і загальна система міжнародної колективної безпеки на регіональних і глобальному рівнях [9]. Тобто мова йде про створення інформаційної зброї, застосування якої з урахуванням рівня інформатизації суспільства і уразливості критично важливих структур може мати руйнівні наслідки, які можна порівняти з дією зброї масового ураження. Очевидно, що такою зброєю можуть скористатися й терористичні, екстремістські або кримінальні угруповання, а також окремі правопорушники.

Таким чином, “універсальність, закритість або знеособленість, можливість широкого транскордонного застосування, економічність і загальна ефективність роблять інформаційну зброю надзвичайно небезпечним засобом дії, причому розробка і застосування такої зброї практично не регулюються нормами сучасного права” [9].

Наведене веде до протидії порушенню вимог і правил інформаційного законодавства, а й отже – до забезпечення інформаційної безпеки.

Взагалі, слід відмітити, що при визначенні змісту поняття “інформаційна безпека” одні юристи-науковці (В.І. Ярочкін, В.П. Сальников) виходять з того, що раніше забезпечення інформаційної безпеки зводилося лише до захисту інформації (державної та службової таємниці), а також ототожнюють два різних поняття – “захист інформації” та “інформаційна безпека”, хоча це зовсім не одне і те ж саме [8, с. 21]. Інші (А. Прохожев, Н. Чуканов), говорячи про інформаційну безпеку, досить часто розуміють цей термін вузько, як набір апаратних і програмних засобів для забезпечення збереження, відкритості та конфіденційності баз даних у комп’ютерних мережах. На їх думку, те, що у 1970-ті роки визначалося терміном “комп’ютерна безпека”, у 1980-ті роки – безпекою даних, на цей час іменується інформаційною безпекою. Інформаційною ж безпекою вони називають “заходи щодо захисту інформації від неавторизованого доступу, руйнування, модифікації, розкриття і затримки в доступі”, при цьому використовується термін “критичні дані”, під якими розуміють дані, що вимагають захисту від вірогідності завдання збитку в тому випадку, якщо відбудеться випадкове чи умисне розкриття, зміна або руйнування даних [4, с. 154]. Третя група учених (В.А. Галатенко, В.К. Льовін) вважає, що стан інформаційної безпеки особи, суспільства і держави визначається, головним чином, двома чинниками: інформаційно-

психологічною задоволеністю потреб громадян і негативними (навмисними або випадковими) інформаційно-психологічними та інформаційно-технічними діями [1, с. 38-43; 3, с. 5-18].

Відповідно до статті 85 Конституції України [2] Верховна Рада України визначає основні напрями внутрішньої і зовнішньої політики, у тому числі і у сфері інформаційної безпеки. Виходячи з аналізу положень Закону України “Про основи національної безпеки України” [7], Доктрини інформаційної безпеки України [5] та Концепції Національної програми інформатизації [6] визначені основні інтереси і загрози в інформаційній сфері, основні завдання і принципи державної політики щодо забезпечення інформаційної безпеки.

Таким чином, інформаційна безпека стає одним з найважливіших елементів національної безпеки. Причому мова йде не тільки про захист баз даних від несанкціонованого доступу, а й про загальні принципи функціонування інформаційних ресурсів держави, захист найважливіших інформаційних і телекомунікаційних систем, що забезпечують діяльність транспорту, енергетики, промисловості, органів державного управління. У широкому сенсі слова інформаційна безпека включає такі проблеми, як протистояння культурній експансії з боку країн з розвиненою аудіовізуальною промисловістю, збереження національної і мовної самобутності. Вагому роль у формуванні в Україні механізмів забезпечення інформаційної безпеки повинна відіграти відповідна концепція протидії інформаційним правопорушенням.

У зв’язку з цим виникає очевидна потреба в міжнародно-правовому регулюванні світових процесів цивільної і військової інформатизації, розробці світової безпеки, що відповідає інтересам, і узгодженої міжнародної платформи з проблеми протидії інформаційним правопорушенням.

Правовою основою подальших зусиль міжнародного співтовариства у цьому напрямі може стати прийнята консенсусом Резолюція 53/70 Генеральної Асамблеї ООН від 4 грудня 1998 року “Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки” [9]. Далі слід ухвалити Генеральною Асамблеєю резолюції з проблеми протидії інформаційним правопорушенням, конкретизовані у частині обмеження викликів і загроз як терористичного або кримінального, так і військового характеру.

Необхідно продовжувати міжнародний розгляд ситуацій у сфері інформаційної безпеки з метою виявлення усіх наявних позицій і поглядів та їх обліку, загального просування спільної міжнародної концепції протидії інформаційним правопорушенням.

Також слід зазначити, що за визначенням загальних підходів і тенденцій протидії інформаційним правопорушенням необхідно розробити міжнародні принципи (режим, кодекс поведінки держав), спрямовані на зміцнення міжнародної інформаційної безпеки, які могли б бути спочатку сформульовані у вигляді багатосторонньої декларації, а в перспективі – закріплені у формі багатостороннього міжнародно-правового документа.

При цьому слід виходити з доцільності розгляду і ухвалення міжнародним співтовариством згаданих принципів у комплексі, тобто з урахуванням викликів і загроз військового, терористичного або кримінального характеру і стосовно як до військових, так і до цивільних сфер.

Аналіз інформаційного законодавства показує, що воно розвивається в двох діалектично зв'язаних напрямах. З одного боку, багато законів, міжнародні угоди спрямовані на зняття обмежень, заохочення конкуренції, створення умов, що сприяли б зростанню інформаційної індустрії. З іншого боку, цю свободу діяльності і самовираження необхідно об’єднати з суспільними інтересами, що виражаються в

обмеженнях на зміст повідомлень у глобальних комп’ютерних мережах, захист прав на недоторканність особистого життя, на інтелектуальну власність тощо.

Соціальна трансформація, що має місце на даному етапі розвитку світового простору, – не стихійний процес. Її результати багато в чому залежать від держави, як одного з головних суб’єктів суспільного процесу. Перехід до інформаційного суспільства, звичайно, залежить і від інших чинників – ступеня розвитку інформаційної інфраструктури, загального технологічного рівня, ступеня розвиненості демократичних інститутів. Проте держава у процесі становлення інформаційного суспільства може і повинна узяти на себе роль каталізатора змін і спрямовувати їх в бажаному для суспільства напрямі. Узгоджена політика держав, таким чином, формуватиме закони, загальні для всіх суб’єктів міжнародного права в інформаційній сфері. При цьому необхідно мати на увазі не лише позитивні аспекти інформаційного суспільства, а й проблеми, що можуть виникнути. Втрата соціальної орієнтації технологічного розвитку може призвести до зворотних і несподіваних ефектів, наприклад, посилення контролю над особою, ще більшій маніпуляції індивідуальною і масовою свідомістю, додаткового поділу суспільства на тих, хто має доступ до інформації, володіє комп’ютерною грамотою, вміє працювати в новому інформаційному оточенні і хто не володіє цими інструментами (життєво необхідними навиками за сьогоднішніх умов). Крім того, необхідно зрозуміти напрям і ступінь державного впливу, що здійснюється шляхом ухвалення законів і нормативно-правових актів, на формування соціально привабливого інформаційного суспільства і міжнародної співпраці у сфері обміну інформацією.

Останнім часом інформаційне законодавство є галуззю права, що інтенсивно модернізується. Це ще одне свідчення на користь того, що суспільство прагне знайти гідну відповідь на стрімкий розвиток інформаційно-телекомунікаційних технологій оскільки багато законодавчих актів виходять з рекомендацій міжнародних організацій і судових рішень.

Далі слід відмітити, що з метою вироблення ефективного механізму протидії інформаційним правопорушенням необхідно виокремити виклики та загрози у сфері міжнародної інформаційної безпеки. До них, на нашу думку, відносяться:

а) створення і використання засобів впливу і завдання збитків інформаційним ресурсам і системам іншої держави;

б) цілеспрямований інформаційний вплив на критично важливі структури іншої держави;

в) інформаційний вплив з метою підриву політичної і соціальної системи держави, психологічна обробка населення з метою дестабілізації суспільства;

г) дії держав, що ведуть до їх домінування і контролю в інформаційному просторі, протидія доступу до новітніх інформаційних технологій, створення умов технологічної залежності у сфері інформатизації за рахунок збитків інших держав;

ґ) дії міжнародних терористичних, екстремістських і злочинних співтовариств, організацій і окремих правопорушників, що представляють загрозу інформаційним ресурсам і критично важливим структурам держав;

д) розробка і ухвалення державами планів, доктрин, концепцій, що передбачають можливість ведення інформаційних воїн і здатних спровокувати гонку озброєнь, а також викликати напруженість у відносинах між державами і, власне, виникнення інформаційних конфліктів;

е) використання інформаційних технологій і засобів за рахунок порушення (обмеження) основних прав і свобод людини, що реалізуються в інформаційній сфері;

є) неконтрольоване транскордонне поширення інформації, що суперечить принципам і нормам міжнародного права, а також внутрішньому законодавству конкретних держав;

ж) маніпулювання інформаційними потоками, дезінформація та приховування інформації з метою спотворення психологічного і духовного середовища суспільства, ерозії традиційних культурних, етичних та естетичних цінностей;

з) інформаційна експансія, придбання монопольного контролю над національними інформаційно-телекомунікаційними інфраструктурами іншої держави, включаючи умови їх функціонування в міжнародному інформаційному просторі.

З урахуванням вказаного вище існує нагальна необхідність формування міжнародно-правової основи для протидії інформаційним правопорушенням за напрямами:

а) визначення ознак і класифікації інформаційних правопорушень, а також інформаційних конфліктів, під якими прийнято розуміти протиборство між державами в інформаційному просторі з метою завдання збитків інформаційним системам, процесам і ресурсам, підриву політичної і соціальної систем іншої держави, а також масованої психологічної обробки населення і дестабілізації суспільства;

б) визначення ознак і класифікації інформаційної зброї, а також методів і засобів, які можна віднести до інформаційної зброї;

в) заборона розробки, розповсюдження і застосування особливо небезпечних видів інформаційної зброї. До такого типу зброї, зокрема, відносять – засоби і методи, що вживаються з метою завдання збитків інформаційним ресурсам, процесам і системам іншої держави, негативного інформаційного впливу на оборонні, управлінські, політичні, соціальні, економічні та інші критично важливі системи;

г) визнання порівнянності застосування інформаційної зброї стосовно критично важливих структур з наслідками застосування зброї масового ураження;

ґ) створення умов рівноправного і безпечного міжнародного інформаційного обміну на основі балансу особи, суспільства і держави;

д) розробка процедури взаємного повідомлення і запобігання транскордонному несанкціонованому інформаційному впливу, а також створення механізму вирішення конфліктних ситуацій в інформаційній сфері;

е) створення міжнародної системи сертифікації технологій і засобів інформатизації (зокрема програмно-технічних) у частині гарантій їх інформаційної безпеки;

є) розвиток системи міжнародної взаємодії правоохоронних органів щодо запобігання та протидії правопорушенням в інформаційній сфері.

Усе це безумовно вимагає створення механізму контролю виконання умов режиму міжнародної протидії інформаційним правопорушенням і гармонізації національних законодавств у частині забезпечення інформаційної безпеки.

Діяльність з протидії інформаційним правопорушенням є цілим комплексом проблем. Враховуючи безперечну необхідність в аналізі всіх аспектів такої діяльності для досягнення чіткого розуміння того, як ці аспекти взаємодіють, міжнародне співтовариство повинне осмислити пройдений етап і виробити нові принципи співробітництва в інформаційній сфері.

Видається за очевидне, що міжнародне співробітництво у сфері міжнародної протидії інформаційним правопорушенням має важливе значення в аспекті ефективного вирішення нових складних проблем, що породжуються інформаційним тероризмом і злочинними елементами.

Зв’язок між інформаційними системами у всьому світі на цей час досяг такого ступеня, що держави знаходяться у потенційній небезпеці, життєво важливі елементи їх інформаційної інфраструктури можуть піддатися електронному нападу з боку правопорушників або терористів. Хоча небезпека такого роду електронного нападу, ймовірно, в даний час невелика, вона зростатиме в майбутньому залежно від того, як державний і приватний сектори будуть широко використовувати комп’ютерні системи, які будуть все більш зв’язані одна з одною. Крім того, оскільки такі системи зв’язані у міжнародному масштабі, дана загроза має транскордонний характер. Тому спроби правопорушників проникнути до інформаційних ресурсів окремої держави з протиправним наміром є проблемою для всіх членів світового співтовариства. У зв’язку з цим необхідно розробити конкретні шляхи, спрямовані на застосування відповідних засобів протидії як на односторонній, так і на багатосторонній основі, за допомогою яких можна було б забезпечити недоторканність та захист від таких нападів заснованої на інформаційних системах життєво важливої інфраструктури.

Забезпечення протидії інформаційним правопорушенням є широкою і складною системою, що охоплює багато чинників і що зачіпає багато різноманітних видів діяльності окремих осіб, утворень, урядів. Хоча ця загальна тема включає аспекти, що пов’язані з міжнародним світом і безпекою, вона також охоплює технічні аспекти, які стосуються глобальних комунікаційних систем, так само як і нетехнічні питання, пов'язані з економічним співробітництвом і торгівлею, правами інтелектуальної власності, дотриманням законності, співпрацею в боротьбі з тероризмом та іншими проблемами. Заходи і програми урядів ні в якому разі не є єдиними належними інструментами, оскільки інформаційна сфера також зачіпає важливі проблеми, що представляють інтерес для окремих осіб, асоціацій, підприємств та інших організацій, що діють у приватному секторі.

Зазначимо, що у періоди збройних конфліктів держави використовують різні методи, пов’язані з інформаційною безпекою. Прикладами є створення радіоперешкод на певних частотах і використання електромагнітних імпульсів для боротьби з супротивником. Ці методи не нові, проте у майбутньому для збройних сил тієї або іншої держави важливе значення матимуть захист їх власних мереж передачі даних та інших заснованих на застосуванні інформаційних систем. Окрім цього, державам-учасникам міжнародного інформаційного простору необхідно мати в своєму розпорядженні потенціал для відновлення ключових інформаційних систем у тих випадках, коли кризові явища перешкоджають належному та стабільному функціонуванню ключових об’єктів комунікації або інших мереж передачі даних у державному і приватному секторах. Протидії інформаційним правопорушенням охоплює також і захист даних, пов’язаних з військовим потенціалом та іншими об’єктами національної безпеки.

У сучасному світі під час активного науково-технічного прогресу створюється і реальна загроза використання досягнень в інформаційній сфері з метою, що не збігається із завданнями підтримки світової стабільності і безпеки, дотримання принципів суверенної рівності держав, мирного врегулювання суперечок і конфліктів, незастосування сили, невтручання у внутрішні справи, поваги прав і свобод людини.

Таким чином, вважаємо, що в сучасних умовах розбудови інформаційного простору до першочергових завдань, які стоять перед державами у межах міжнародного співробітництва у сфері протидії інформаційним правопорушенням відносяться:

– недопущення використання новітніх інформаційних технологій для розповсюдження соціально шкідливих ідей і закликів, расизму, шовінізму, радикального націоналізму;

– правовий захист національної культури і мови від впливу домінуючих в інформаційному розвитку держав;

– знаходження соціально прийнятного балансу між свободою слова і розповсюдженням інформації та невід’ємним правом держави забезпечувати незалежну політику “інформаційного невтручання” у внутрішні справи іншої держави, як з боку компаній, що використовують факсимільний зв’язок та мережу Інтернет для маркетингу і реклами, так і політичних партій та суспільних рухів, що ведуть пропаганду;

– правове регулювання систем шифрування громадянами для використання при передачі особистих повідомлень за допомогою інформаційних технологій;

– захист від дифамації за допомогою ЗМІ та Інтернету.

Висновки.

Підсумовуючи викладене, слід зазначити, що міжнародне співробітництво з протидії інформаційним правопорушенням за своїм змістом передбачає, з одного боку, нівелювання небезпеки, з іншого – підтримання стану захищеності життєво важливих інформаційних інтересів людини, суспільства, держави від різного роду викликів та загроз. Отже, налагодження належного міжнародного співробітництва у сфері забезпечення інформаційної безпеки є необхідною умовою життєдіяльності світового інформаційного простору. Потребують подальшого формулювання рекомендації як з належного застосування міжнародних інформаційно-правових норм, так і з їх удосконалення з урахуванням сучасних реалій функціонування інформаційного простору.

Використана література

1. Галатенко В.А. Основы информационной безопасности : учеб. пособ. / В.А. Галатенко ; под ред. акад. РАН Бетелина В.Б. – М. : “Интернет-университет информационных технологий”, 2006. – 208 с.

2. Конституція України від 28.06.96 р. № 254/96 ВР // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

3. Левин В.К. Защита информации в информационно-вычислительных системах и сетях // Программирование. – 1994. – № 5. – С. 5-18.

4. Мелюхин И.С. Информационное общество : истоки, проблемы, тенденции развития / И.С. Мелюхин. – М. : МГУ, 1999. – 208 с.

5. Про Доктрину інформаційної безпеки України : Указ Президента України від 08.07.09 р. № 514/2009 // Офіційний вісник України. – 2009. – № 20. – С. 18. – Ст. 677.

6. Про Концепцію Національної програми інформатизації : Закон України від 04.02.98 р. № 75/98-ВР // Відомості Верховної Ради України. – 1998. – № 27. – Ст. 182.

7. Про основи національної безпеки України : Закон України від 19.06.03 р. № 964-IV // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

8. Ярочкин В.И. Информационная безопасность : учеб. пособ. / В.И. Ярочкин. – М. : МГСУ. – 2000. – 400 с.

9. Distr. General A/54/213 10 August 1999. – Режим доступу : //www.sussex.ac.uk/.../UN% 20A54218_Adv%20

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