раны промышленной собственности. – Одесса, 1897. – 117 с.; *Казанский П. Е*. Международный союз для печатания таможенных тарифов. – Одесса, 1897. – 36 с.; *Казанский П. Е.* Международный союз железнодорожных товарных сношений. – Одесса, 1897. – 156 с.; *Казанский П. Е*. Международный союз книговедения. – Одесса, 1897. – 40 с.; *Казанский П. Е.* Международный союз мер и весов. – Одесса, 1897. – 69 с.

[19] *Казанский П. Е*. Всеобщие административные союзы государств. – Т. 1. – Одесса, 1897. – С. 7.

[20] Там само. – С. 8.

[21] Там само. – С. 33.

[22] *Грабарь В. Э*. Война и международное право // Академічна юридична думка. – К., 1998. – С. 201–212.

[23] Див.: Савчук К. О. Грабар В. Е. Про війну та мир в міжнародних відносинах // Актуальні проблеми міжнародних відносин: Збірник наукових праць. – Вип. 22. – Ч. 2. – К., 2000. – С. 137–144; *Савчук К. О*. Міжнародно-правові погляди академіка В. Е. Грабаря. – К., 2003. – С. 87–94.

[24] *Казанский П. Е.* Всеобщие административные союзы государств. – Т. 1. – Одесса, 1897. – С. 53.

[25] Там само. – С. 54.

[26] Див.: *Савчук К. О*. Концепція права міжнародного управління професора П. Є. Казанського та її значення для сучасної науки міжнародного права // Наукові читання, присвячені пам'яті В. М. Корецького: Збірник наукових праць. – К., 2011. – С. 75–79.

[27] *Казанский П. Е*. Всеобщие административные союзы государств. – Т. 1. – Одесса, 1897. – С. 67.

[28] Там само. – С. 68.

[29] Там само. – С. 172.

[30] *Мартенс Ф. Ф*. Современное международное право цивилизованных народов. Т. 1. – М., 2008. – С. 18–24.

[31] *Казанский П. Е*. Всеобщие административные союзы государств. – Т. 1. – Одесса, 1897. – С. 277–278.

[32] Детальніше про це див.: *Савчук К. О*. Концепція права міжнародного управління професора П. Є. Казанського та її значення для сучасної науки міжнародного права // Наукові читання, присвячені пам'яті В. М. Корецького: Збірник наукових праць. – К., 2011. – С. 76–77.

[33] *Казанский П. Е.* Всеобщие административные союзы государств. – Т. 1. – Одесса, 1897. – С. 279.

[34] Там само. – С. 327.

[35] Там само. – С. 500–502.

[36] Там само. – С. 514.

[37] Там само. – С. 514.

Резюме

У цій статті досліджуються міжнародно-правові погляди відомого вітчизняного юриста-міжнародника XIX – початку XX сторіччя Петра Євгеновича Казанського.

Ключові слова: історія міжнародного права, історія науки міжнародного права, П. Є. Казанський.

Резюме

В этой статье исследуются международно-правовые взгляды известного отечественного юриста-международника XIX – начала XX столетий Петра Евгеньевича Казанского.

Ключевые слова: история международного права, история науки международного права, П. Е. Казанский.

Summary

This article is devoted to analysis international-legal thoughts of well-known domestic international lawyer of the XIX – beginning of XX centuries PetroYevhenovych Kazansky.

Key words: history of international law, history of international-legal science, Kazansky P. Y.

Отримано 19.10.2011

М. М. НАГОРНЯК

Михайло Миколайович Нагорняк, *доктор політичних наук, професор Прикарпатського національного університету ім. В.Стефаника*

ВПЛИВ США І РОСІЇ НА ФОРМУВАННЯ МІЖНАРОДНО-ПРАВОВОЇ БАЗИ У СФЕРІ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Розвиток інформаційно-комунікаційних технологій (ІКТ) створив умови для організації принципово нових засобів комунікації в політиці, науці, бізнесі та повсякденному спілкуванні. Проте наслідки такого

бурхливого розвитку глобальних мереж привели до неоднозначної ситуації: з одного боку, не можна не відзначити ті нові можливості, котрі сприяють компаніям і державам ефективніше вирішувати економічні, соціальні і політичні питання, а з другого – проблеми, породжені змінами в інформаційній галузі, пов'язані з можливістю застосування нових технологій у цілях, не сумісних із завданням забезпечення міжнародної стабільності й безпеки.

Вороже використання інформаційно-комунікаційних технологій на рівні держав щодо інформаційних інфраструктур іншої держави в політичних, у тому числі військових цілях, злочинна діяльність у кіберпросторі стали предметом дослідження А. В Крутських[1], О. Б. Озерова[2], І. Н. Панаріна[3], А. А. Стрельцова[4], А. В. Федорова[5] та ін.

Оскільки віртуальний простір не має географічних кордонів, то, на думку дослідників, інформаційна зброя стала важливим елементом військового потенціалу держав, котрий не тільки ефективно доповнив існуючий арсенал традиційного озброєння, а й призвів до зміни форм міждержавних конфліктів.

Підкресливши важливість таких проблем, треба відзначити, що за допомогою інформаційно-комунікативних технологій може здійснюватися не тільки дестабілізація економіки, підрив суверенітету і основ державного устрою, порушення нормального функціонування практично всіх інфраструктур держави, в тому числі критично важливих, а й транскордонно можуть здійснюватися напади й агресії без залучення армійських підрозділів і військової техніки, руками недержавних суб'єктів. Очевидним є той факт, що в умовах існування глобального взаємозв'язку національних інформаційних просторів, жодна із держав, навіть з тих, що є лідерами в галузі інформаційних технологій, не в змозі самостійно розв'язати проблеми своєї інформаційної безпеки. Тому слід визнати те, що які б кроки із захисту свого національного інформаційного ресурсу не здійснювалися провідними державами, їхні дієвість і ефективність залежать від рівня захищеності інформаційних просторів інших держав[6]. Саме тому проблема міжнародно-правового забезпечення міжнародної інформаційної безпеки займає важливе місце в зовнішньополітичній діяльності США і Росії.

Слід зазначити, що в ході переговорного процесу кожна із держав послідовно відстоює свою позицію в питаннях інформаційної безпеки, яка найбільше відповідає її національним інтересам. Тому розробка правової бази в цій сфері відбувається повільно і непросто, незважаючи на наявні прецеденти. Мається на увазі прийняті раніше міжнародні договори і конвенції у високотехнологічних галузях: Договір про принципи діяльності держав з дослідження і використання космічного простору, включаючи Місяць та інші небесні тіла (1967), Конвенція з морського права (1982) та ін.).

У статті проаналізовано складний договірний процес кодифікації діяльності в нових технологічно важких і вкрай чутливих для національної безпеки сферах, показано його поетапність і пошуки прийнятних форм та принципів діяльності держав у сфері міжнародної інформаційної безпеки.

Аналізуючи вплив держав на вироблення міжнародно-правового режиму у сфері міжнародної інформаційної безпеки, варто зазначити ряд факторів, котрі мають неабиякий вплив на позиції держав у переговорному процесі. Перш за все це наявна перевага США в інформаційних технологіях, ресурсний потенціал Росії, відсутність норм міжнародного права, які містили би чіткі обмеження на застосування інформаційної зброї та жорстка боротьба за геополітичне лідерство.

Відчуваючи свою перевагу в інформаційних технологіях, США прагне використати їх для посилення свого політичного, економічного, культурного і військового впливу, що відповідає її стратегії однополярного світу. При цьому використовуючи своє становище і вплив у цілому ряді міжнародних організацій, таких як Організація економічного співробітництва і розвитку (ОЕСР), ООН, «велика вісімка», Рада Європи, Організація американських держав (ОАД), США безпосередньо впливають на розробку основоположних принципів захисту критичної інфраструктури. У 1992 р. ОЕСР було прийнято документ «Керівні принципи по безпеці інформаційних систем і мереж», де зазначено, що забезпечення безпеки інформаційних мереж є важливим завданням для всього міжнародного співтовариства, оскільки вони не обмежуються рамками національних кордонів. У документі визначено основні загрози безпеки – віруси, хакери, а також співробітники компаній, котрі навмисне заподіюють шкоду інформаційним системам. Методами захисту інформаційних систем названо перевірки та ідентифікацію користувачів, контроль за доступом до файлів і контроль за мережами[7]. Саме цей документ, котрий визначив вектор розвитку міжнародного співробітництва у сфері захисту інформаційних систем, також відіграв важливу роль у розвитку глобальної культури кібербезпеки і визначив позиції держав у міждержавному діалозі. Вже в ході підготовки до самміту «Росія – США» у 1998 р. російською стороною було запропоновано проект спільної заяви президентів з проблем інформаційної безпеки, в якій містився пакет превентивних заходів протидії глобальним загрозам. Цим самим було зроблено спробу включити США до обговорення питання військової складової інформаційної безпеки, але американська сторона обмежилась вербальною заявою про те, що проект прийнято до відома[8].

Небажання США підтримати висловлені російською стороною ініціативи змусило її шукати інших шляхів впливу. При цьому тактика поведінки Росії будувалася на реальній оцінці переваг США не тільки в інформаційних технологіях, а й їх впливу на міжнародні організації. Тому з огляду на це, Російська Федерація вирішила посилити свої позиції щодо прийняття рішень з питань інформаційної безпеки в ООН.

У своєму листі від 1 жовтня 1998 р. міністр іноземних справ Російської Федерації І. Іванов звернувся з посланням до Генерального секретаря ООН Кафі Аннана, в якому підкреслювалося, що інформаційна зброя своїм руйнівним ефектом не поступається зброї масового знищення, а інформаційні війни є загрозою міжнародній безпеці. До послання додавався проект резолюції Генеральної Асамблеї ООН (далі – ГАООН), в ос-

нову якого лягли ідеї концепції міжнародної безпеки, що були вироблені в ході роботи Міжвідомчої комісії Ради безпеки Росії. Просуваючи свої ініціативи з міжнародної інформаційної безпеки, російська сторона розраховувала на те, що підготовлений проект резолюції буде прийнятий на ГАООН Першого комітету в 1999 р. У ньому містилися вимоги щодо вироблення міжнародних правових режимів із розробки, виробництва і використання інформаційної зброї, а також створення міжнародної системи моніторингу загроз щодо боротьби з інформаційним тероризмом і криміналітетом. Просування російських ініціатив означало втрату ініціативи в США у цьому питанні, а тому, посилаючись на відсутність опрацьованої теоретичної і понятійної бази для детального розгляду проблемних питань, американська сторона підкреслила, що порушені питання не є компетенцією Першого комітету ГАООН, котрий займається питаннями роззброєння і міжнародною безпекою, і виступила за перенесення розгляду цього питання у Другий (комітет з економічних і фінансовий питань) і Шостий (комітет з правових питань) комітети ГА ООН. На думку США, порушена в резолюції тема відображає технічні аспекти, пов'язані з економічним співробітництвом і торгівлею інтелектуальною власністю, правоохоронною діяльністю, боротьбою з тероризмом та іншими питаннями, що відповідає компетенції даних комітетів. Крім того, на їх думку, не слід фокусуватися виключно на діях урядів та їхніх програмах, оскільки ця ініціатива також зачіпає суттєві інтереси осіб, підприємств та інших організацій у приватному секторі[9].

Шість років поспіль (аж до 2005 р.) російська резолюція з проблем міжнародної інформаційної безпеки приймалась ГА ООН на основі консенсусу. За цей час її розширено і конкретизовано новими положеннями, котрі відповідали ідеям міжнародної стабільності та безпеки. 1 грудня 1999 р. ГАООН було прийнято оновлену резолюцію «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки» (54/49). У ній вперше було чітко окреслено тріаду загроз міжнародній інформаційній безпеці: загрози застосування інформаційно-комунікаційних технологій у військових, терористичних і злочинних цілях.

У цьому самому руслі Міністерством закордонних справ Росії було підготовлено і направлено до Секретаріату ООН документ «Принципи, що стосуються міжнародної інформаційної безпеки». П'ять базових принципів міжнародної інформаційної безпеки визначають роль права, зобов'язання і відповідальність держав в інформаційному просторі, окреслюють конкретні завдання, вирішення яких було би спрямовано на обмеження загроз у сфері міжнародної інформаційної безпеки, а також визначають роль ООН у даному контексті. Закладені в них моральні зобов'язання держав стали свого роду робочим варіантом проекту кодексу поведінки інформаційного простору і заклали основу для широких міжнародних переговорів під егідою ООН із цієї проблематики[10].

Порушені російською стороною питання міжнародної безпеки змусили США визнати, що державами використовуються різні методи, пов'язані з інформаційною безпекою: створення радіоперешкод на певних частотах і використання електромагнітних імпульсів для боротьби з супротивником. Одночасно відзначалося, що в майбутньому для збройних сил тієї чи іншої держави важливе значення матиме не тільки захист їх власних комп'ютерних мереж, а й наявність у держав необхідного потенціалу для відновлення ключових інформаційних мереж у випадку стихійного лиха або надзвичайних ситуацій[11].

Особливий акцент американською стороною було зроблено на терористичній діяльності, котра розглядалась як головна загроза міжнародній інформаційній безпеці. Враховуючи високий рівень глобальної взаємозалежності й взаємозв'язку інформаційних систем, США вважають за необхідне як в односторонньому, так і в багатосторонньому порядку сприяти впровадженню належних заходів для забезпечення безпеки ресурсів, використання яких залежить від застосування інформаційних технологій. Що до запропонованих Російською Федерацією принципів міжнародної інформаційної безпеки, то США вважають, що їх вироблення можливе лише після того, як будуть проаналізовані всі аспекти інформаційної безпеки, що дасть можливість скласти чітку картину їх взаємодії[12].

Відзначаючи значущість міжнародного співробітництва для ефективного розв'язання нових і складних проблем, породжених інформаційним тероризмом, США на противагу Росії виступили за активізацію роботи з розв'язання таких проблем у рамках міжнародних форумів, таких як Рада Європи, «велика вісімка», ОАД. Втягування Генеральної Асамблеї ООН у розробку будь-яких стратегій або конкретних заходів, на думку США, могло би не тільки завадити, а й завдати шкоди роботі, що проводиться ними[13].

Така постановка питання відповідала реальним крокам, зробленими ОЕСР, «великою вісімкою» та Радою Європи із вироблення керівних принципів з безпеки міжнародних систем і мереж та основ міжнародного законодавства в сфері кіберзлочиності. Саме ці напрацювання лягли в основу «Окінавської хартії глобального інформаційного суспільства», прийнятої країнами «великої вісімки», Конвенції із кіберзлочинності Ради Європи і резолюції ООН A/res/57/239 «Створення глобальної культури кібербезпеки».

На зустрічі лідерів країн «великої вісімки» в Окінаві у 2000 р. було прийнято Хартію глобального інформаційного суспільства. У ній зокрема підкреслюється, що «інформаційно-комунікаційні технології є одним із найбільш важливих факторів, які впливають на формування суспільства двадцять першого століття»[14]. Разом з тим зусилля міжнародного співтовариства щодо розвитку цього суспільства мають супроводжуватися узгодженими діями зі створення безпечного і вільного від злочинності кіберпростору[15]. Керуючись принципами безпеки інформаційних систем ОЕСР від 1992 р., країни визнали за необхідне здійснити ефективні заходи боротьби із злочинами в комп'ютерній сфері[16]. Документ передбачає розширення співробітництва країн «великої вісімки» в рамках Ліонської групи щодо транснаціональної організованої злочинності. Використання досвіду роботи Ліонської групи, в якій працює група боротьби з високотехно-

логічними злочинами, дає змогу визначити стратегію і політику щодо підвищення ефективності боротьби з міжнародною злочинністю і тероризмом.

Варто відзначити, що країни «великої вісімки» розробили практичний механізм щодо боротьби з кіберзлочинами, що діє 24 год протягом семи днів тижня. Цей механізм сприяє обміну інформацією між учасниками групи з високотехнологічних злочинів[17].

Проблемами боротьби зі злочинами у сфері високих технологій, починаючи з кінця 1980-х р., займається Рада Європи. Ще до появи російських ініціатив у 1995 р. нею були прийняті Рекомендації з боротьби з кіберзлочинами, в яких зокрема містилася вимога поліпшити міжнародну співпрацю з цих питань. У 1997 р. в рамках Ради Європи було створено Комітет експертів зі злочинів у кіберпросторі, який розробив проект Міжнародної конвенції з боротьби з кіберзлочинністю. 23 листопада 2001 р. на конференції у Будапешті держави–члени Ради Європи підписали Конвенцію із кіберзлочинності (*Convention on Cybercrime*), до якої приєдналися США, Канада, Японія і ПАР.

Не маючи належного впливу в названих міжнародних форумах, Росія продовжувала активно використовувати ООН для відстоювання своїх позицій щодо проблем міжнародної безпеки, котрі відповідали її національним і геополітичним інтересам. Відповідно до рекомендацій резолюції 55/28 в Секретаріат ООН російською стороною було направлено новий документ «Загальна оцінка проблем інформаційної безпеки. Загрози міжнародній інформаційній безпеці». Цей документ був включений в доповідь Генерального секретаря ООН A/56/164/Add від 3 жовтня 2001 року. У ньому було викладено та описано одинадцять факторів, що створюють, на думку керівництва Російської Федерації, небезпеку основним інтересам особи, суспільства і держави в інформаційному просторі. До таких факторів були віднесені перш за все розробка і використання засобів несанкціонованого втручання в роботу і неправомірного використання інформаційних ресурсів іншої держави; цілеспрямований інформаційний вплив на критичні інфраструктури і населення іншої держави; діяння, спрямовані на домінування в інформаційному просторі; заохочення тероризму і власне ведення інформаційних війн[18].

На думку США, загроза цілісності й працездатності національної і глобальної інформаційної інфраструктури здебільшого випливає з неправомірних дій у кіберпросторі, а не спричинена військовими діями одних держав проти інших[19]. Тому питання використання «інформаційної зброї» та «інформаційних війн», котрі відображено у підготовлених російською стороною документах, трактувалися США та їх союзниками як злочинні діяння, спрямовані проти інформаційних структур і мереж та оцінювалися як терористичні акти[20].

У світлі подій 11 вересня 2001 р. акцент у позиції США на терористичній діяльності посилився. У 2002 р. Організацією економічного співробітництва і розвитку були прийняті нові «Керівні принципи щодо безпеки інформаційних систем і мереж». У документі визначено поняття «культура безпеки» («*culture of sekurity*») як новий спосіб мислення і поведінки під час використання інформаційних систем і мереж та взаємодія всередині них, за якої особливу увагу приділяють аспектам безпеки[21]. Основні положення цього документа лягли в основу резолюції ООН A/RES/57/239 «Створення глобальної культури кібербезпеки», прийнятої 20 грудня 2002 р. Резолюція довела до відома всіх держав основоположні принципи, котрими слід керуватися при взаємодії з інформаційними системами[22]. Після прийняття Резолюції США продовжили роботу в рамках Другого комітету з питань створення глобальної культури кібербезпеки. Результатом цієї роботи стала Резолюція A/RES/58/199 «Створення глобальної культури кібербезпеки і захист найважливіших інформаційних структур», прийнята на 58-й сесії ГАООН.

Враховуючи відсутність у міжнародному праві норм, котрі гарантували би міжнародну інформаційну безпеку, США взяли активну участь у розробці Конвенції з кіберзлочинності, що містить керівні принципи для національних законодавчих систем і міждержавного співробітництва у сфері діяльності правоохоронних органів. У даній Конвенції сторони визнають необхідність співробітництва між державами в боротьбі з кіберзлочинністю. Згідно зі ст. 25, Сторони на взаємній основі здійснюють одна одній за можливості максимальну правову допомогу у проведенні розслідування або судового розгляду кримінальних злочинів, пов'язаних з комп'ютерними мережами і даними, або збиранням доказів щодо кримінального злочину в електронній формі[23]. Крім того, ст. 35 Конвенції передбачає створення механізму співробітництва між державами з метою ефективнішого розкриття кримінальних злочинів. «Кожна Сторона визначає контактний центр, котрий працює 24 год на добу сім днів на тиждень, щоб забезпечити надання невідкладної допомоги при розкритті або судовому розслідуванні кримінальних злочинів, котрі мають відношення до комп'ютерних систем і даних»[24].

Правові норми Конвенції є обов'язковими для імплементації в національне законодавство держав-учасниць і значно розширюють повноваження урядів при розслідуванні звичайних злочинів, скоєних за допомогою комп'ютерних мереж. У Конвенції піднято питання про гармонізацію законодавчої бази з питань боротьби з кіберзочинністю. Законодавством кожної країни-учасниці вчинення таких дій, як неавторизований доступ до комп'ютера, незаконне перехоплення даних, викрадення і заподіяння шкоди даним, розглядається як правопорушення[25]. Варто зауважити, що держави-учасниці використали досвід Ради Європи і «великої вісімки» щодо створення механізму контролю і обміну інформацією у питаннях кіберзлочинності та кібербезпеки.

Таким чином, Конвенція розглядається США як модель при розробці національного законодавства з боротьби з комп'ютерними злочинами для країн, котрі не підписали її. Разом з цим при всій актуальності про-

блеми гармонізації законодавчої бази у питаннях боротьби із кіберзлочиністтю простежується намагання США взяти участь у діяльності міжнародних організацій для просування своїх національних інтересів у сфері інформаційної безпеки на глобальному рівні. Крім того, не можна не відзначити ще однієї особливості використання для переговорного процесу плацдарму міжнародних форумів ОЕСР та «великої вісімки», адже в їх рамках не зачіпаються питання військового застосування інформаційно-комунікаційних технологій, що відповідає підходам США до проблеми міжнародної інформаційної безпеки.

На думку Росії, саме військовий аспект використання інформаційних засобів і технологій за своєю значущістю є найбільш важливим і небезпечним з точки зору потенційних наслідків застосування інформаційної зброї. Тому дана проблематика просувалася Росією як в ООН, так і по лінії міжнародних форумів[26].

Важливим з політичної і дипломатичної точки зору стало прийняття резолюції 56/19 на 56-й сесії ГА-ООН 29 листопада 2001 р. про створення в 2004 р. спеціальної групи урядових експертів-членів ООН для вивчення проблеми міжнародної інформаційної безпеки. Російське бачення організаційно-практичної діяльності цієї групи та можливі пріоритети її роботи були викладені в «Питаннях, пов'язаних з роботою групи урядових експертів з проблеми інформаційної безпеки». Цей документ А /58/373 від 13 вересня 2003 р. увійшов у доповідь Генерального секретаря ООН.

З прийняттям резолюції з інформаційної безпеки (58/32) ГАООН від 8 грудня 2003 р. відбувся перехід від загальнополітичного обговорення проблеми міжнародної інформаційної безпеки до запуску механізму формування групи урядових експертів. Створення групи урядових експертів відбулося на основі принципу географічного розподілу, що забезпечило участь у ній урядових експертів Російської Федерації, США, Великобританії, Франції, Китаю, Німеччини, Білорусії, Бразилії, Мексики, Йорданії, ПАР, Малі, Індії, Малайзії, Республіки Корея. Позиція російського експерта базувалася на пошуках шляхів і засобів зниження військової загрози міжнародній інформаційній безпеці, а тому вимагала вироблення групою політичної оцінки і правового механізму гарантій безпеки, тоді як американський експерт у групі наполягав на зосередженні зусиль експертів виключно на технологічних аспектах захисту інформаційних мереж.

Свою політичну і правову оцінку міжнародної інформаційної безпеки Росія відстоювала на ряді міжнародних форумів, зокрема по лінії Всесвітньої зустрічі на вищому рівні з питань інформаційного обміну (перший етап – 10–12 грудня 2003 р., Женева, другий етап – 16–18 листопада 2005 р., Туніс), на 16-й Повноваженій конференції Міжнародного союзу електрозв'язку в м. Марракеш (Марокко 23 вересня – 18 жовтня 2002 р.), на засіданні Ради Шанхайської Організації Співробітництва (ШОС) 15 червня 2006 р.

Вироблений Групою експертів держав – членів ШОС план дій із забезпечення міжнародної інформаційної безпеки, затверджений Рішенням Ради глав держав – членів цієї організації 18 серпня 2007 р., передбачав вироблення єдиного понятійного апарату сфери міжнародної інформаційної безпеки, вивчення і порівняльний аналіз національних законодавств у сфері забезпечення інформаційної безпеки, координацію позицій держав – членів ШОС у рамках міжнародних форумів і організацій, дослідження питання про міжнародно-правове регулювання і стан міжнародно-правової бази сфери міжнародної інформаційної безпеки та ін.[27].

Отже, робота над виробленням договірної бази відбувалася поетапно з паралельним прийняттям загальних принципів діяльності держав у відповідних галузях. У разі, коли з тих чи інших причин неможливо було досягнути згоди щодо суворо зобов'язальних договорів, були найдені нові прийнятні форми: міжнародний кодекс поведінки, керівні принципи, меморандуми про наміри. Саме ці типи документів можна було би використовувати як основу багатостороннього договору (конвенції), що створює універсальний режим міжнародної інформаційної безпеки. Згідно з таким договором держави та інші суб'єкти міжнародного права повинні будуть нести міжнародну відповідальність за діяльність в інформаційному просторі і за її відповідність його основним положенням.

---

[1] *Крутских А. В.* Информационный вызов безопасности на рубеже XXI века / А. В. Крутских // Международная жизнь. – 1999. – № 2. – С. 82–89.

[2] *Озеров О. Б.* Дипломатия в эпоху информационных технологий / О. Б. Озеров // Международная жизнь. – 1997. – № 4. – С. 55–60.

[3] *Панарин И. Н.* Информационная война и власть / И. Н. Панрин. – М.: Мир и безопасность, 2001. – 456 с.

[4] *Стрельцов А. А.* Обеспечение информационной безопасностим России: Теоретические и методологические основы / Под ред. В. А. Садовничева и В. П. Шерстюка. – М.: МЦНМО, 2002. – 536 с.

[5] *Крутских А. В.* О международной информационной безопасности / А. В. Крутських, А. В. Федоров // Международная жизнь. – 2000. – № 2. – С. 37–48.

[6] *Поляков Ю. А.* Информационная безопасность и средства массовой информации : учебное пособие / Ю. А. Поляков. – [Електронний ресурс] – Режим доступу: http://cjes.ru/lib/content.php?content_id=6692

[7] Guidelines for the Security of Information System, 26 November 1992 [Електронний ресурс] – Режим доступу: http://www.oecd.org/document/19/0,2340,en_2649_34255_1815059_1_1_1_1,00/html

[8] *Коновалов А.* Инфомационная безопасность: кто – за, кто – против ?/ А. Коновалов // Современная Европа. – 2003. – № 2. – С. 65.

[9] *Richard W.* Aldrich Guberterrorism and Computer Crimes: Issues Surrounding the Establishment of an International Legal regime. INSS Occasional Paper 32. Information Operations Series. April 2000 [Електронний ресурс] – Режим доступу: http: // www.au.af.mil/au/aul/bibs/infowar/if.htm.

[10] Информационные вызовы национальной и международной безопасности / Под. общ. ред. А. В. Федорова и В. Цыгичко. – М.: Библиотека ПИР-Центра, 2001. – С. 120–123.

[11] Доклад Генерального секретаря ООН A/54/213, 10 августа 1999 г. [Електронний ресурс] – Режим доступу: http://www.un.org/russian/documen/gadocs/54 sess/reslcte.htm

[12] Там само.

[13] Там само.

[14] Okinawa Charter on Global Information Society. Okinawa, 23 July 2000. [Електронний ресурс] – Режим доступу: http://europa.eu.int/cjmm/external_relations/g7g8/intro/ global_info_society.htm.

[15] Там само.

[16] Там само.

[17] Там само.

[18] *Цыгичко В. Н*. Информационное оружие и международная информационная безопасность / В. Н. Цыгичко, Д. С. Вотрин, А. В. Крутских, Г. Л. Смолян, Д. С. Черешкин. – М.: Ин.-т системного анализа РАН, 2001. – С. 257–264.

[19] US Comments on March 21 WSIS Draft Declaration and Action Plan– [Електронний ресурс] – Режим доступу: http://www.state.gov/e/eb/cip/wsis

[20] Коновалов А. Инфомационная безопасность: кто – за, кто – против? / А. Коновалов // Современная Европа. – 2003. – № 2. – С.66.

[21] OECD Guidelines for the Security of Information Systems and Networks, 25 July 2002. [Електронний ресурс] – Режим доступу: http://www.oecd.org/dataoecd/16/22/15582260.pdf.

[22] Statement by Michele Markoff, State Departament Senior Coordinator for International Critical Infrastructure Protection Policy, on the Introduction of draft resolution “Creation of a Clobal Culture of Cybersecurity” in the Second Committee, October 24, 2002. [Електронний ресурс] – Режим доступу: http://www.un.int/usa/02_167.htm.

[23] Convention on Cybercrime, 23 November 2001. [Електронний ресурс] – Режим доступу: http://conventions.coe.int /Treaty/en/Treaties/Html/185.htm.

[24] Там само.

[25] Там само.

[26] *Крутских А. В*. О международной информационной безопасности / А. В. Крутских, А. В. Федоров // Международная жизнь. – 2000. – № 2. – С. 37–48.

[27] Инновационные направления современных международных отношений: учеб. пособие для студентов вузов / А. В. Бирюков, Е. С. Зиновьева, А. В. Крутских и др.; под ред. А. В. Крутских и А. В. Бирюкова. – М.: Аспект Пресс, 2010. – 295 с.

Резюме

У статті аналізовано договірний процес кодифікації діяльності США і Росії у нових технологічно складних і вкрай чутливих для національної безпеки сферах, висвітлено його поетапність і пошуки прийнятних форм та принципів діяльності держав у сфері міжнародної інформаційної безпеки.

Ключові слова: інформаційно-комунікаційні технології, інформаційна безпека, кіберпростір, зовнішньоекономічна діяльність.

Резюме

В статье анализируется договорной процесс кодификации деятельности США и России в новых технологически сложных и достаточно ощутимых для национальной безопасности сферах, показана его поэтапность и поиски принятных форм и принципов деятельности государств в сфере международной информационной безопасности.

Ключевые слова: информационно-коммуникационные технологии, информационная безопасность, киберпространство, внешнеэкономическая деятельность.

Summary

This article analyzes the contractual process of codification of the United States and Russia in the new technologically complex and high sensitive to national security areas, it is shown its order and searches of acceptable forms and principles of the states in the field of international information security.

Key words: information and communication technologies, information security, cyberspace, foreign economic activity.

Отримано 12.10.2011