Олександр Білоусов
Одеський національний політехнічний університет, Україна

МІЖНАРОДНЕ ВРЕГУЛЮВАННЯ МЕРЕЖІ ІНТЕРНЕТ ЯК АДЕКВАТНА ВІДПОВІДЬ НА СВІТОВІ ІНФОРМАЦІЙНІ ЗАГРОЗИ

Oleksandr Bilousov
Odesa National Polytechnic University, Ukraine

INTERNATIONAL REGULATION OF THE INTERNET AS ADEQUATE ANSWER FOR GLOBAL INFORMATION THREATS

This article aims to study international legal regulation of the Internet. Analysis of modern international legal norms and recommendations on mass media in Europe allows to set that they are based on principles of self-regulation of their activity, minimization of state control and limits on distribution of information in the Internet, impossibility of limitations for content in the Internet, more than limitations for other media (in particular, concentrated on that a row of the documents accepted by Council of Europe in resolution № 1120 «about influence of new communicative and informing technology on democracy» (in 1997), «declaration about European policy in industry of new information technology» (in 1999), «declaration about freedom of communication in the Internet» (in 2003), and so on.

Key words: Internet, information technology, legal regulation, European convention, mass media, world threats.

В останній час стійкою тенденцією для більшості країн світу стало намагання державних органів посилити контроль за точками доступу до мережі Інтернет (зокрема інтернет-кафе) та інтернет-трафіком громадян. Особлива увага з боку правоохоронних органів приділяється контролю за контентом у соціальних мережах, блогах тощо.

Останнє цілком закономірно, адже останніми роками саме ці сучасні засоби спілкування на базі новітніх ІКТ широко використовувалися соціально-політичними протестними рухами при поваленні кількох політичних режимів, зокрема, у країнах Арабського Сходу. Разом з тим, на думку багатьох фахівців, їх роль у цих подіях сильно перебільшена.

Так, з січня 2011 року країни Магрибу та Близького Сходу захлеснула небувала хвиля соціальних протестів, що призвела за собою відставку режимів в одних країнах, репресії упереміж з гарячковими реформами в інших, а подекуди – громадянську війну і фактичний крах державності. Ці події стали відомі як Арабська весна і Twitter / Facebook-революції. Друга із згаданих назв відображає рису, характерну для більшості епізодів близькосхідних протестів, – безпрецедентно активне використання учасниками протестів інформаційно-комунікаційних технологій (ІКТ), і в першу чергу соціальних мережевих сервісів. Дослідник цих процесів О. Дємідов цілком справедливо підкреслює, що Арабська весна закріпила в рядах політиків, експертів і ЗМІ дискурс ІКТ (і, перш за все, соцмережі) як фактор хвилювань і революцій. Невинна технологія, покликана спростити спілкування на дозвіллі, набула рис чи не зброї масового знищення, що загрожує стабільності і безпеці окремих країн і міжнародного співтовариства в цілому. Суперечки про роль соціальних мереж в Арабській весні сьогодні визначають основну суть дискусії навколо них, однак коло пов'язаних з ними питань в рамках проблематики безпеки, звичайно ж, набагато ширше [1].

О. Дємідов, висловлюючи не лише свою думку, але й узагальнюючи погляди інших авторитетних фахівців цієї галузі, приходить до висновку, що «Соціальні мережеві сервіси, як і інші продукти ІКТ, самі по собі не є і не можуть бути джерелом і причиною соціальних хвилювань і тим

[1] Демидов, О. (2011). Социальные сетевые сервисы в контексте международной и национальной безопасности. *Индекс безопасности, 4 (99), том 17,* 59–76.

більше революцій. Більш того, соціальні мережі не оформилися і в якості недержавних акторів, подібним ТНК, які чітко усвідомлювали б свої інтереси і можливі стратегії в подіях, подібних Арабській весні. … Роль соціальних мереж в соціально-політичних трансформаціях також не буває ні монопольної, ні переважаючою серед інших засобів комунікації. Відповідно, розгляд соціальних мереж як можливої загрози або виклику міжнародній та національній безпеці позбавлене сенсу і стало б класичним прикладом помилкової проблеми» [1].

Іншої думки дотримується ціла низка сучасних авторів, які безпосередньо залучені владою до інформаційного протиборства. Вони стверджують, що вже давно розпочата справжня мережева війна. Так, наприклад, В. Коровін характеризує її так: «Мережева війна, що називається також «війною шостого покоління», – це технологія перемоги в ситуації, коли противник навіть не в змозі скористатися своїм озброєнням для відбиття агресії, у тому числі ядерним арсеналом. Війна ведеться настільки непомітно, а перемога настільки стрімка і очевидна, що ніяка навіть найбільш сучасна зброя та військова техніка не знаходять собі застосування у цій війні» [2].

Аналіз сучасних міжнародних правових норм і рекомендацій щодо Інтернет-ЗМІ в Європі дозволяє констатувати, що вони ґрунтуються на принципах стимулювання саморегуляції їхньої діяльності та мінімізації державного контролю і обмежень на поширення інформації в Інтернеті, неможливості встановлення обмежень для контенту в Інтернеті, більших, ніж обмеження для інших меіа (зокрема, на цьому зосереджена низка документів, прийнятих Радою Європи – Резолюція № 1120 «Про вплив нових комунікативних та інформаційних технологій на демократію» (1997 р.), «Декларація про Європейську політику в галузі нових інформаційних технологій» (1999 р.), «Декларація про свободу комунікацій в Інтернеті» (2003 р.) [3].

Спираючись на аналіз значного масиву актів Європейського Союзу щодо забезпечення інформаційної безпеки, О. О. Смірнов приходить до обґрунтованого висновку, що «вибудувана система забезпечення інформаційної безпеки в ЄС забезпечує здатність адекватного реагування на основні типи ризиків та загроз віртуалізації. Меншою мірою у порівнянні з іншими вибудувані компоненти протидії загрозам маніпуляції суспільною свідомістю і застосування інформаційної зброї» [4].

Водночас, аналіз європейського досвіду у даній сфері свідчить, що в міжнародних правових нормах, які визнають більшість європейських країн, значна увага приділяється протидії розповсюдженню протизаконного контенту в мережі Інтернет. Так, зокрема, в прийнятому Європейським Союзом «Плані заходів щодо забезпечення безпечного користування Інтернетом» (від 01 січня 1998 року) надається тлумачення поняттям «матеріали протизаконного змісту» та «матеріали засудливого змісту».

Під матеріалами протизаконного змісту розуміються такі, що мають відношення: до національної безпеки (інструкції з виготовлення вибухових пристроїв, з незаконного виробництва наркотиків, інструкції з проведення терористичних акцій); до захисту неповнолітніх (образливі форми маркетингу, сцени насильства, порнографія); до захисту людської гідності (підбурювання до расової ненависті або расової дискримінації); до економічної безпеки (шахрайство, інструкції по піратському використанню кредитних карток); до захисту інформації (діяльність злочинних хакерів); до захисту приватного життя (недозволена передача персональних даних, електронне переслідування); до захисту репутації (наклеп у пресі, незаконна порівняльна реклама); до інтелектуальної власності (недозволене поширення творів, захищених авторським правом, наприклад, комп'ютерних програм або музичних творів).

Під матеріалами засудливого змісту розуміються такі, що не є протизаконними, проте поширення яких обмежене (наприклад, тільки для дорослих), а також зміст, яких може образити деяких користувачів, хоча їх опублікування не обмежене в силу принципу свободи самовираження [5].

[1] Демидов, О. (2011). Социальные сетевые сервисы в контексте международной и национальной безопасности. *Индекс безопасности, 4 (99), том 17,* 74.

[2] Коровин, В. (2014). *Третья мировая сетевая война*. Санкт-Петербург: Питер, 24.

[3] Конах, В.К. Інтернет-ЗМІ в Україні: проблеми визначення нормативно-правового статусу та врегулювання діяльності. *Аналітична записка*. <http://www.niss.gov.ua>

[4] Смирнов, А.А. (2012). *Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза.* Москва: ЮНИТИ-ДАНА, 110.

[5] Конах, В.К. Інтернет-ЗМІ в Україні: проблеми визначення нормативно-правового статусу та врегулювання діяльності. *Аналітична записка*. <http://www.niss.gov.ua>

З огляду на зазначене, відносно цих двох категорій застосовуються зовсім різні заходи. Так, матеріалами протизаконного змісту займаються, за місцем їх створення, правоохоронні органи, дії яких регулюються національними законодавствами та угодами про судову співпрацю. Що ж стосується матеріалів засудливого змісту, то перш за все, слід надати користувачам можливості самим вирішувати проблему виключно технічними засобами (за допомогою систем фільтрації та рейтингової оцінки змісту), підвищуючи батьківську обізнаність і розвиваючи саморегулювання, здатне створити необхідні рамки, зокрема у відношенні захисту неповнолітніх [1].

Радою Європи ще в 1989 році була прийнята перша Рекомендація з питань кіберзлочинності. За нею в 1995 році з'явилась друга Рекомендація з питань кіберзлочинності, що стосується процесуальних аспектів проблеми. У ній же вже висувалася ідея розробки міжнародного договору з кіберзлочинності. Оцінивши ту загрозу, яку містить у собі розростання цього явища, Європейський комітет з проблем злочинності доручив науковому світу вивчити проблему і запропонував розробити Конвенцію, в котрій розглядалися б не тільки питання позитивного права щодо протидії кіберзлочинності, а й процесуальні вимоги до вирішення цієї проблеми.

Йдеться про прийняту Радою Європи у 2001 році Конвенцію про кіберзлочинність (її ж називають також за містом прийняття Будапештською Конвенцією з кіберзлочинності). Вона охоплює широке коло питань, зокрема всі аспекти кіберзлочинності, включаючи незаконний доступ до комп'ютерних систем і перехоплення даних, вплив на дані та на роботу системи, протизаконне використання пристроїв, підроблення та шахрайство з використанням комп'ютерних технологій, правопорушення, пов'язані з дитячою порнографією, та ті, що порушують авторські і суміжні права. Також, при підготовці конвенції переслідувалися цілі формування загальної правоохоронної системи для протидії кіберзлочинності і створення умов для обміну інформацією між усіма країнами, які підписали конвенцію.

Безпосередньо до сфери кіберзлочинів європейська Конвенцію про кіберзлочинність відносила такі: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ до комп'ютерної системи або її частини; нелегальне перехоплення комп'ютерних даних; втручання в комп'ютерні дані; втручання у комп'ютерну систему; зловживання пристроями); правопорушення, пов'язані з комп'ютерами (підробка, пов'язана з комп'ютерами; шахрайство, пов'язане з комп'ютерами); правопорушення, пов'язані зі змістом (правопорушення, пов'язані, наприклад, з дитячою порнографією); правопорушення, пов'язані з порушенням авторських та суміжних прав [2].

У Комюніке Європейської комісії «На шляху до спільної політики по боротьбі з кіберзлочинністю» кіберзлочинність визначається як комплексне поняття, що охоплює три категорії кримінальних дій: традиційні види злочинів (шахрайство, підробка документів і т. п.), що здійснюються з використанням електронних комунікаційних мереж та інформаційних систем; розміщення незаконного контенту в електронних медіа; атаки проти інформаційних систем, блокування програмного забезпечення сайтів та хакерство [3].

Україна ратифікувала європейську Конвенцію про кіберзлочинність 2001 р. у 2005 році відповідним Законом [4]. Крім того, у 2006 році Україна також ратифікувала додатковий протокол до Конвенції, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи [5].

Водночас далеко не всі країни (з-поміж тих, що входять до Ради Європи) ратифікували цей документ. Так, на сьогодні Конвенцію підписали 47 країн, але ратифікували її лише 33 країни.

[1] Конах, В.К. Інтернет-ЗМІ в Україні: проблеми визначення нормативно-правового статусу та врегулювання діяльності. *Аналітична записка*. <http://www.niss.gov.ua>

[2] Конвенція про кіберзлочинність. *Офіційний сайт Верховної Ради України.* <http://zakon2.rada.gov.ua>.

[3] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions – Towards a general policy on the fight against cyber crime {SEC(2007) 641} {SEC(2007) 642}. <http://eur-lex.europa.eu/legal-content/EN/ALL/;ELX_SESSIONID=GMMjJYlc1P94DDmmw1TTvFnVsVTQnQJDW0TGL9dFdzvzskjWmQ25!-283335449?uri=CELEX:52007DC0267>.

[4] Закон про ратифікацію Конвенції про кіберзлочинність 2005 (Верховна Рада України). *Офіційний сайт Верховної Ради України.* <http://zakon3.rada.gov.ua/laws/show/2824-15>.

[5] Закон про ратифікацію Конвенції про кіберзлочинність 2005 (Верховна Рада України). *Офіційний сайт Верховної Ради України.* <http://zakon3.rada.gov.ua/laws/show/2824-15>.

Важливо зазначити, що до країн, які не підписали конвенцію, увійшли Австрія, Бельгія, Грузія, Чехія, Російська Федерація та інші. До того ж, вказаний документ є регіональним (хоча до нього долучаються й інші країни світу) і не вирішує питань воєнного використання кіберпростору, глобальних міжнародних підходів до кібербезпеки тощо.

Тому цілком природно, що для того, щоб заповнити цей правовий вакуум на глобальному рівні висуваються відповідні ініціативи з боку, перш за все, провідних геополітичних гравців – США, Російської Федерації, того ж таки Європейського Союзу та інших.

Головна зовнішньополітична ініціатива США щодо перспектив розвитку кіберпростору була оприлюднена 16 травня 2011 р. під назвою Міжнародна стратегія для кіберпростору (International Strategy for Cyberspace, далі – Стратегія). Цей документ не лише визначає принципові положення, якими будуть керуватися США при формуванні власної політики щодо кіберпростору, а й окреслює «очікуване майбутнє», яке вони планують побудувати в кіберпросторі. Так, «базовими принципами», що мають бути забезпечені при формуванні політики щодо кіберпростору, Стратегія визначає:

• «Фундаментальні свободи» (можливість шукати, отримувати й передавати інформацію та ідеї через будь-які засоби зв'язку, незважаючи на кордони).

• «Прайвесі» (люди мають бути обізнані з загрозами їхній персональній інформації та про можливість здійснення проти них кіберзлочинів).

• Вільні потоки інформації» (рух інформації не має обмежуватися фільтрами, міжмережевими екранами, оскільки вони створюють видимість безпеки, кіберпростір має бути місцем інновацій та співпраці держави й бізнесу задля більшої безпеки [1].

Цим документом установлено риси бажаного майбутнього в кіберпросторі для США. Особливий інтерес у контексті даного розділу дисертації становлять положення, що стосуються міжнародного регулювання (або бачення в цілому) кіберпростору.

З цього приводу у документі виділено три стратегічні цілі, яких має досягти реалізація американської Стратегії:

1. Відкритість і сумісність. Зростання цифрових систем має поступово привести до здешевлення доступу до кіберпростору дедалі більшої кількості людей. Для розвитку впроваджувані інновації мають бути сумісними між собою, а також більш активно використовувати програмне забезпечення з відкритим кодом. Це дозволить створювати системи з єдиною логікою використання для всіх регіонів світу. Альтернатива цьому процесу є неприйнятною, оскільки передбачає фрагментування мережі Інтернет, де через особливі політичні інтереси держав великим групам людей буде заборонений доступ до сучасного контенту. Відповідно пріоритетом тут є розроблення нових інформаційних технологій, які засновані на міжнародних, загальноприйнятих стандартах, що забезпечить зростання цифрової економіки і рух суспільства вперед.

2. Безпека й надійність. Користувачі мають впевнитись у безпеці своїх даних. Забезпечення подібного стану – завдання поліаспектне й таке, що потребує загальної відповідальності на всіх рівнях суспільства (починаючи від простих користувачів і закінчуючи державними органами) та ефективної міждержавної співпраці. Головним питанням тут є встановлення міжнародних технічних стандартів (щодо програмного й апаратного забезпечення й систем управління інцидентами) та узгоджених міжнародних норм поведінки держав. Це потребуватиме розширення співпраці в питаннях обміну технічною інформацією з приватним сектором і міжнародним співтовариством. Оскільки головним елементом надійності є безпека мереж, США готові інвестувати в них не лише на національному рівні, а й сприяти більшій надійності мереж за кордоном.

3. Стабільність через норми. Цей пункт становить особливий інтерес, оскільки дозволяє в цілому зрозуміти американське бачення чинного міжнародного правового поля щодо кібер простору і орієнтирів його трансформації. Відповідно до тексту Стратегії, вироблення єдиних правил поведінки у кіберпросторі – головне завдання, й тому США готові працювати над виробленням консенсусної точки зору з приводу того, що таке «прийнятна поведінка» і «партнерство» в кіберпросторі. Відповідно до тексту Стратегії, «вироблення таких норм сприятиме передбачуваності поведінки держав, що дозволить попереджувати конфліктні ситуації чи непорозуміння». США не бачать необхідності приймати принципово нові міжнародні документи, оскільки чинне міжнародне

[1] International Strategy for Cyberspace. <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>

законодавство не є «застарілим» відносно реалій кіберпростору: «розроблення правил поводження держави у кіберпросторі не потребує оновлення чинного міжнародного законодавства та не робить існуючі міжнародні норми застарілими. Багаторічні міжнародні норми, що визначають дії держави під час миру та війни, також стосуються кіберсередовища». Водночас визнається необхідність певного доопрацювання міжнародних норм [1].

Головним пріоритетом для США залишається Будапештська Конвенція з кіберзлочинності. Цей документ, на думку авторів Стратегії, має стати базовим для всіх подальших напрацювань у сфері вироблення норм поведінки в кіберпросторі. Про це свідчить і те, що розділ «Розширення співробітництва та верховенство права» (ст. 19–20 Стратегії) значною мірою присвячено саме вказаній Конвенції. Зокрема зазначається, що США розглядає важливе питання «подальші дискусії щодо міжнародних норм» протидії кіберзлочинності в першу чергу як проблему «поширення чинних зусиль, таких як Будапештська конвенція» на всіх учасників.

Крім того, зазначається, що докладатимуться зусилля до налагодження двосторонньої співпраці між державами. Другий пункт цього розділу вказує на необхідність узгодження національних нормативно-правових документів у сфері протидії кіберзлочинності з Будапештською конвенцією, яка, на думку авторів Стратегії, «є моделлю для розроблення та оновлення чинних законів» у цій сфері. США зі свого боку зобов'язуються стимулювати інші країни приєднуватися до Конвенції [2].

Цілком ймовірно, як прогнозують аналітики, що у випадку довгострокового інтересу США до просування Будапештської конвенції в якості основного документа для багатостороннього співробітництва, будуть здійснюватися зусилля з трансформації цього документа у своєрідний міжнародний договір.

При цьому, США надто широко у порівнянні зі Статутом ООН та резолюцією 3314 (XXIX) Генеральної Асамблеї ООН від 14 грудня 1974 р. щодо визначення агресії, трактують два пункти – «право на самозахист» і «надійний доступ» (а також пов'язаний із ним пункт про «додержання основних свобод»), що вряд чи може бути підтримано багатьма іншими державами і, в першу чергу, КНР.

У таких умовах видається сумнівним, що кібератака, згідно з чинними міжнародними документами, може кваліфікуватись як «агресія» чи «напад» і, тим більше, тягнути за собою право на військову відповідь. Незважаючи на це, у Стратегії безпосередньо йдеться саме про те, що США готові застосовувати «дипломатичні, інформаційні, військові й економічні» засоби для реагування на подібні інциденти. У який спосіб цитоване положення може бути реалізоване на практиці у площині міжнародного права без внесення кардинальних змін до Резолюції ООН, щодо визначення «агресії» на даний час залишається незрозумілим. Наразі існують лише окремі наукові напрацювання у сфері міжнародного права, які пропонують або визнати кіберзброю зброєю масового знищення, або (що виглядає більш реалістично) виробити механізм оцінки наслідків від здійснення кібератак та порівнювати їх із можливими наслідками від застосування традиційних озброєнь.

Щодо офіційної позиції США, то інший важливий аспект, пов'язаний із запропонованою моделлю поведінки держав по відношенню до Всесвітньої мережі, визначається вимогами «надійний доступ» та «додержання основних свобод». У Стратегії цій проблемі присвячено розділ «Інтернет-свобода: підтримуючи фундаментальні свободи та прайвесі». У ньому містяться чотири основних напрями зусиль США з щодо вирішення даного питання.

1. Підтримка громадянського суспільства в питаннях отримання надійних і безпечних платформ для забезпечення свободи слова та зібрань. США закликають усіх до максимально активного використання цифрових засобів зв'язку задля обміну думками, інформацією, моніторингу виборів, боротьби із корупцією, організацію суспільних і політичних рухів та засудження тих, хто переслідує, арештовує чи погрожує тим людям, які користуються цифровими засобами. США готові сприяти розширенню прав і можливостей громадянського суспільства, правозахисників і журналістів використовувати такі цифрові засоби, а також сприяти тим урядам, що «вирішують реальні загрози у кіберпросторі, а не нав'язують компаніям обов'язки щодо обмежень свободи слова

[1] International Strategy for Cyberspace. <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>

[2] International Strategy for Cyberspace. <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>

чи вільних потоків інформації».

2. Співробітництво з громадянським суспільством і неурядовими організаціями щодо підвищення їх кібербезпеки (зокрема, їх електронних поштових адрес, веб-сайтів, мобільних телефонів тощо).

3. Сприяння міжнародному співробітництву для більш ефективного захисту комерційних конфіденційних даних.

4. Забезпечення наскрізної сумісності систем, що задіяні в передачі інформації у мережі Інтернет [1]

Своєрідним продовженням проблематики даної Стратегії та її органічним розвитком і доповненням стали засадничі тези, оприлюднені тодішнім держсекретарем США Гілларі Клінтон під час конференції «Свобода інтернету», що відбулась 8 грудня 2011 р. у м. Гаазі (Нідерланди). У своєму тривалому виступі, віддаючи належне тематиці «основних свобод» та Інтернету, держсекретар США розкритикувала практику затримання блогерів – громадських активістів (цей закид стосувався, переусім, РФ) та практику китайського уряду, пов'язану з укладанням спеціальних угод із компаніями, що надають телекомунікаційні послуги, коли останні вдаються до самоцензури та самообмежень. Заяви Гілларі Клінтон з приводу необхідності врегулювання даного питання цілком логічно слідували запропонованому Стратегією формату забезпечення положень про «фундаментальні права». До того ж, у тексті цієї промови було піднято ще три додаткових проблеми, які стосуються довгострокових стратегічних планів США щодо кіберпростору, а саме:

1. Приватний сектор має прийняти свою роль у захисті Інтернет свободи. Це означає, на думку Гілларі Клінтон, що приватні компанії, що торгують технологіями, які можуть бути використані для придушення «свободи слова» (системи спостереження, моніторингу інтернет трафіку тощо), мають фактично вдаватися до самоцензури при обранні клієнтів для своєї продукції й не чекати на відповідні рішення Держдепартаменту.

2. Недопущення використання урядами тематики «управління інтернетом» з метою посилення «контролю за інтернетом».

3. Створення коаліції за «відкритий Інтернет». Дане положення практично означає заклик держав до об'єднання у коаліцію, що не допустить обмежень мережі в окремих країнах. У більш широкому сенсі США виступають категорично проти будь-яких бар'єрів у кіберпросторі, що можуть тлумачитися як своєрідні кордони держави в кіберпросторі, і створення такої коаліції – лише один з інструменів вирішення цього питання.

Головна ідея вказаного виступу Гілларі Клінтон полягає у рішучому запереченні зв'язку даної проблеми (правового регулювання Інтернету) з питаннями безпеки (протидії кіберзлочинності, розповсюдження дитячої порнографії, кібертероризмом), наголошуючи, що проблеми мають вирішуватись у інший правовий спосіб, не порушуючи «динамізму розвитку Мережі» [2].

Що стосується перспектив перетворення задекларованої США Стратегії у дійсно загальновизнаний міжнародний документ (або ж, принаймні, такий, що ляже у його основу), то вони видаються досить проблематичними через те, що на сьогодні Стратегія не знайшла загальносвітової підтримки. Закладений в неї підхід поділяє в основному більшість європейських країн і частина країн Східної півкулі (наприклад, Японія, Австралія, Нова Зеландія). Це підтверджується тим, що деякі з цих країн вже на практиці розпочали інтенсивну двосторонню співпрацю із США на даному напрямі.

З іншого боку, як вже зазначалося, існує низка держав, які не зможуть прийняти запропоновану США Стратегію в повному обсязі принципову незгоду з кількома її позиціями. Таким чином, враховуючи, що США акцентують увагу в просуванні Конвенції, можна припустити, що результативної дискусії тут найближчим часом не відбудеться.

По-друге, теза про «вільні потоки інформації», що не можуть обмежуватись за будь-яких умов національними урядами, принципово не співпадає із поглядом деяких інших країн на те, яким чином можуть бути використані ці інформаційні потоки (зокрема, для дестабілізації політичної, економічної та соціальної ситуації в країні). Частина пояснень тези про «вільні потоки» (наприклад, щодо активної підтримки з боку США громадянського суспільства у всьому світі) ще більше

[1] International Strategy for Cyberspace. <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>

[2] Свобода Інтернету. Виступ держсекретаря США Гілларі Клінтон під час конференції 8 грудня 2011 р. у м. Гаазі. <http://ukrainian.ukraine.usembassy.gov/uk/clinton-intfreedom2011.html>.

переконує уряди цих країн у неможливості прийняти подібне твердження як базове.

По-третє, малоймовірно, що США, з одного боку, та доволі широка коаліція держав – з іншого, зможуть прийти до дійсно консолідованої точки зору щодо проблеми управління Інтернетом. США однозначно займають позицію щодо продовження підпорядкованості контролю за мережею Інтернет корпорацією ICANN. Незважаючи на цілий ряд дій, що були здійснені керівництвом корпорації для позбавлення іміджу компанії, яка безпосередньо підпорядкована уряду США, більшість країн світу продовжують наполягати на передачі її повноважень та функцій спеціально створеному органу під егідою ООН.

При цьому, варто взяти до уваги, що держави – опоненти США, у свою чергу, не займають позицію пасивного неприйняття запропонованої США Стратегії, але й виходять на міжнародну арену з ініціативою власних, альтернативних їй документів аналогічної функціональної спрямованості. Основна концептуальна відмінність, що вирізняє ці альтернативні проекти від американської ініціатив, – фактична відсутність розділення кібербезпеки з більш широким (а іноді й доволі абстрактним) поняттям «інформаційно-психологічної безпеки».

Так, наприклад, КНР послідовно відстоює позицію, що кібербезпеку не можна розглядати як повністю самостійний напрям, який існує окремо від соціальних, політичних, економічних і військових наслідків застосування сучасних інформаційних технологій. Більше того, за такого підходу (згідно зазначеної позиції) взагалі недоречно казати про абсолютно «вільні потоки інформації», оскільки безпекова тематика охоплює й наслідки їх впливу на державу та її громадян. Отже, казати про «кібербезпеку» (навіть у міжнародному контексті) не зовсім вірно, в той час як більш адекватною назвою даної проблеми є «інформаційна безпека» чи «міжнародна інформаційна безпека», яка і названа загрозою нумер один у сучасному політичному просторі.

References:

1. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions – Towards a general policy on the fight against cyber crime {SEC(2007) 641} {SEC(2007) 642}. <http://eur-lex.europa.eu/legal-content/EN/ALL/;ELX_SESSIONID=GMMjJYlc1P94DDmmw1TTvFnVsVTQnQJDW0TGL9dFdzvzskjWmQ25!-283335449?uri=CELEX:52007DC0267>. [in English].
2. Demidov, O. (2011). Social'nye setevye servisy v kontekste mezhdunarodnoj i nacional'noj bezopasnosti [Social networking services in the context of international and national security]. *Indeks bezopasnosti [Security Index], 4 (99), vol. 17,* 59–76. [in Russian].
3. International Strategy for Cyberspace. <http://www.whitehouse.gov/sites/default/files/rss_ viewer/international_strategy_for_cyberspace.pdf> [in English].
4. Konakh, V.K. Internet-ZMI v Ukraini: problemy vyznachennia normatyvno-pravovoho statusu ta vrehuliuvannia diialnosti [Internet Media in Ukraine: the problem of definition of legal status and regulation activity]. *Analitychna zapyska [Analytical note]*. <http://www.niss.gov.ua> [in Ukrainain].
5. Konventsiia pro kiberzlochynnist [Convention on Cybercrime]. *Ofitsiinyi sait Verkhovnoi Rady Ukrainy [Official website of the Verkhovna Rada of Ukraine]*. <http://zakon2.rada.gov.ua>. [in Ukrainain].
6. Korovin, V. (2014). *Tret'ja mirovaja setevaja vojna [Third World network war]*. Saint-Petersburg: Piter. [in Russian].
7. Smirnov, A.A. (2012). *Obespechenie informacionnoj bezopasnosti v uslovijah virtualizacii obshhestva. Opyt Evropejskogo Sojuza [Ensuring information security in society virtualization. The experience of the European Union.].* Moscow: JuNITI-DANA. [in Russian].
8. Svoboda Internetu. Vystup derzhsekretaria SShA Hillari Klinton pid chas konferentsii 8 hrudnia 2011 r. u m. Haazi [Internet freedom. Statement by US Secretary of State Hillary Clinton during a conference Dec. 8, 2011 in the Hague]. <http://ukrainian.ukraine.usembassy.gov/uk/clinton-intfreedom2011.html>. [in Ukrainain].
9. *Zakon pro ratyfikatsiiu Konventsii pro kiberzlochynnist 2005 [The Law on Ratification of the Convention on Cybercrime in 2005]* (Verkhovna Rada of Ukraine). *Ofitsiinyi sait Verkhovnoi Rady Ukrainy [Official website of the Verkhovna Rada of Ukraine].* <http://zakon3.rada.gov.ua/laws/show/2824-15>. [in Ukrainain].