

– протягом останніх десятиліть, як свідчать результати досліджень, спостерігається тенденція до поширення інформаційної агресії і насилля;

– практично на кожному кроці нам нав’язуються агресивна реклама, спроби маніпуляції свідомістю людини, періодично проводяться інформаційно-психологічні операції;

– за оцінками американських експертів майже у 120 країнах світу проводяться розробки інформаційної зброї або її елементів. Для порівняння – розробки зброї масового знищення здійснюються у близько 20 країнах;

– вчені та експерти європейських країн, України, Росії та США зазначають, що наслідки використання сучасної інформаційної зброї можуть бути співставними із застосуванням зброї масового ураження;

– це становить реальну загрозу безпеці всього людства та міжнародному правопорядку.

Враховуючи зазначене проблема інформаційного виміру колективної безпеки є вкрай важливою для більшості країн світу, які розвивають або формують інформаційні суспільства.

При цьому виникає низка системних проблем, які потребують опрацювання, зокрема:

– перегляду принципів та механізмів міжнародного співробітництва в галузі безпеки з урахуванням глобальних інформаційних тенденцій;

– пошуку балансу між правами людини і потребою держав та суспільства у забезпеченні інформаційної безпеки;

– посилення міжнародно-правової відповідальності за використання в інформаційній сфері сил і засобів, які створюють загрози життю і здоров’ю людини;

– розробки сучасних моделей інформаційної безпеки.

Учасники “круглого столу” констатували, що зазначене потребує подальшого комплексного та системного опрацювання.

Матеріали “круглого столу” опубліковано окремим збірником:

Моделі колективної безпеки: інформаційний вимір : збірник матеріалів. – [Упорядник Ланде Д.В.]. – К. : НДЦПІ НАПрН України. – 2011. – 96 с.

~~~~~ \* \* \* ~~~~~

### **Міжнародна конференція від 26 травня 2011 року на тему:**

## **“ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ І БЕЗПЕКА. ПРОБЛЕМИ НАУКОВОГО І ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КИБЕРБЕЗПЕКИ В СУЧАСНОМУ СВІТІ”**

26 травня 2011 року Інститутом проблем реєстрації інформації НАН України, Науково-дослідним центром правової інформатики НАПрН України і Національним інститутом стратегічних досліджень при Президентові України була проведена Міжнародна конференція на тему “Інформаційні технології і безпека. Проблеми наукового і правового забезпечення кібербезпеки в сучасному світі”.

На порядок денний було винесене обговорення проблем глобалізації інформаційних систем і їх впливу на формування інформаційного суспільства, проблем безпеки особи, суспільства і держави, включаючи питання інформаційного забезпечення і інформаційної безпеки, нормативно-правового забезпечення, технологій і засобів формування суспільної свідомості.

В ході дискусії учасники обмінялися думками щодо низки актуальних проблем колективної безпеки. Було звернуто увагу на деякі ключові проблеми інформаційної безпеки в сучасних умовах глобалізації, зокрема йшлося про наступне:

Більшість держав світу активно модернізує власні сектори безпеки відповідно до викликів сучасності, особливо зважаючи на потенціал використання мережі Інтернет у воєнних цілях. Цей процес відбувається паралельно з активним реформуванням систем управління відповідним сектором безпеки (створення спеціалізованих підрозділів, управлінських структур), впорядкуванням нормативного поля, що має забезпечити цілісність державної політики в даній сфері, активною роз'яснювальною роботою серед населення щодо небезпек кіберзагроз, збільшенням чисельності підрозділів, зайнятих у системі кіберзахисту, розробленням кіберзброї та проведенням пробних військово-розвідувальних акцій у кіберпросторі, посиленням контролю за національним інформаційним простором (способами доступу, контентом тощо).

З огляду на заяви високопосадовців США та експертів, задіяних у підготовці нової Стратегічної концепції НАТО щодо необхідності розглядати кібернапади на критично важливу інфраструктуру як “акт війни”, що підпадають під статтю 5 Північноатлантичного договору, варто очікувати посилення дискусії на найвищому міжнародному політичному рівні (ОБСЄ, керівні органи НАТО, Генеральна Асамблея та Рада безпеки ООН, саміти Великої вісімки) щодо можливості закріплення відповідних змін у міжнародно-правових актах та статутних документах провідних міжнародних безпекових організацій. Це дозволить ідентифікувати кібернапади або їх сукупність як акти війни. Існує цілком реальний ризик, що спроби ототожнення кібератак з “актами війни” можуть бути реалізовані на практиці. В такому разі Україна може опинитися в двозначній ситуації і стати об'єктом додаткового впливу з боку деяких держав як потенційне джерело небезпеки для критичної інфраструктури розвинених держав світу (через активність українських хакерів на міжнародній арені).

Тенденція посилення контролю з боку правоохоронних органів за контентом національного інформаційного простору, за мережевим трафіком, засобами доступу до всесвітньої мережі тощо свідчить про довгострокову тенденцію формування в мережі Інтернет класичних прав і обов'язків громадянина та держави, що існують в державі, та формування своєрідних “цифрових суверенітетів”. Розглядаючи зазначену тенденцію разом із можливістю зменшення рівня анонімності у всесвітній мережі (із введенням Інтернет-паспорту для користувачів), можна зазначити, що панівний до останнього часу неоліберальний підхід до розуміння мережі Інтернет зазнає кардинальних змін, а заступає її “технореалізм” з його ставленням до ІКТ як “технологій подвійного призначення” та ключовою роллю держави у розвитку мережі Інтернет.

Незважаючи на декларовані бажання основних геополітичних суб'єктів протидіяти милітаризації кіберпростору, можна констатувати збільшення ролі суто військових структур у забезпеченні безпеки національної критично важливої інфраструктури (національного кіберпростору). Швидше за все, ініціативи в межах ООН щодо вироблення комплексних підходів до міжнародної інформаційної безпеки будуть або повністю невдалими, або обмежено вдалими (на рівні декларативної згоди). Україна має бути готова не лише до ведення оборонних воєн, а й активно створювати власні наступальні засоби ведення війни в кіберпросторі.

Питання цивільної та воєнної безпеки у кіберпросторі останнім часом дедалі більше ототожнюються. Під тиском військових чинників у всьому світі спостерігається тенденція до напрацювання норм національного та міжнародного права, які не лише регулюють поведінку різних державних та недержавних, військових та невійськових суб'єктів у кіберпросторі, а й безпосередньо стосуються тих специфічних ситуацій, що окреслюються поняттям “кібервійна”. Спостерігається подальша політизація (із спробами переведення в офіційний військовий дискурс) метафоричних понять кібертероризму та кібервійни. Вже в найближчій перспективі це може стати додатковим напрямом у спробах маніпулювання державною політикою.

Вітчизняні реалії кібербезпекової сфери свідчать про низку важливих проблем, що заважають створити ефективну систему протидії загрозам у кіберпросторі. До таких проблем належать передусім: термінологічна невизначеність, відсутність належної координації

діяльності відповідних відомств, залежність України від програмних і технічних продуктів іноземного виробництва, складнощі з кадровим наповненням відповідних структурних підрозділів.

Незважаючи на наявність цілої низки чинних нормативно-правових документів щодо проблем забезпечення безпеки кіберпростору держави, вони не охоплюють усього спектра сучасних загроз кібербезпеці держави.

У чинній нормативно-правовій базі відсутні визначення (а відповідно і не реалізовані особливі форми захисту, реагування та відповідальності) ключових елементів державної інфраструктури саме від кібератак.

Матеріали “круглого столу” опубліковано окремим збірником:

*Информационные технологии и безопасность. Проблемы научного и правового обеспечения кибербезопасности в современном мире : зб. научных трудов за материалами международной научной конференции ИТБ-2011. – (Киев, 26 мая, 2011 г.) – Вып. 11. – К.: ИПРИ НАН Украины, 2011. – 120 с.*

~~~~~ \* \* \* ~~~~~

“Круглий стіл” від 15 вересня 2011 року на тему:

“ТЕОРІЯ І ПРАКТИКА РОЗВИТКУ ІНФОРМАЦІЙНОГО ПРАВА УКРАЇНИ”

15 вересня 2011 року Науково-дослідним центром правової інформатики спільно з Державним комітетом телебачення і радіомовлення України та Українським інститутом підвищення кваліфікації працівників телебачення, радіомовлення і преси “Укртелерадіопресінститут” проведено “круглий стіл” на тему “Теорія і практика розвитку інформаційного права України”.

На порядок денний було винесено обговорення актуальних проблем та пріоритетних напрямів розвитку правової науки в інформаційній сфері в умовах розбудови інформаційного суспільства та інтеграції України у світовий інформаційний простір.

У роботі “круглого столу” взяли участь представники профільного комітету і зацікавлених підрозділів Апарату Верховної Ради України, Державного комітету телебачення і радіомовлення України, Українського інституту підвищення кваліфікації працівників телебачення, радіомовлення і преси, МВС, Служби безпеки та інших державних органів, вчені НАПрН України, а також працівники Науково-дослідного центру правової інформатики НАПрН України.

В ході дискусії учасники обмінялися думками щодо актуальних проблем та пріоритетів розвитку інформаційного права та інформаційного законодавства що стосуються розвитку правової системи України в умовах становлення європейського правового простору, захисту прав та свобод людини і громадянина у сфері ЗМІ, правової охорони та захисту прав інтелектуальної власності в процесі гармонізації національного законодавства, проблеми забезпечення інформаційної безпеки в Україні в умовах розбудови інформаційного суспільства та інтеграції України у світовий інформаційний простір тощо.

Учасники “круглого столу” констатували:

– актуальність проблеми розвитку інформаційного права в умовах становлення інформаційного суспільства та інтеграції України у світовий інформаційний простір,

– потребу вдосконалення інформаційного законодавства України та системи забезпечення безпеки людини і громадянина, суспільства і держави в інформаційній сфері,