Шемчук Віктор Віторович,
кандидат юридичних наук

ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ПРАВ ЛЮДИНИ В УМОВАХ КІБЕРЗАГРОЗ

Розглядаючи проблематику національної безпеки та міжнародної безпеки в сучасних умовах не можливо не згадати про інформаційну безпеку. Звісно, йдеться про її різновиди в якості міжнародної інформаційної безпеки, національної інформаційної безпеки, наднаціональної інформаційної безпеки тощо.

Водночас, не існувало б ймовірно таких категорій, якби не виникали і продовжують виникати ризики і загрози в даній сфері. З-поміж таких в останні роки можна виділити кібератаки, кібервійни, інші форми протиборства у цій сфері. Зокрема, кібервійна розпочинається у кіберпросторі з використання інформаційно-комунікаційних технологій, однак вона може дуже швидко перекинутися за межі віртуального світу, створюючи загрозу урядам, бізнес-середовищу та індивідам.

На жаль, чітких уявлень про згадані категорії сучасною наукою не розроблено, проте спостерігається певна увага світової спільноти, окремих держав до даних питань, результатом чого стало правове регулювання їх окремих аспектів.

Співпраця держав у кіберпросторі покликана базуватися на принципах розумного стримування та обмеження розвитку кіберпотужностей. В основу універсального міжнародно-правового договору має бути покладена добровільна відмова держав від використання кіберозброєння, що може вкрай руйнівні наслідки. Аналогічні домовленості на міжнародному рівні поширення ядерної, хімічної та біологічної зброї. Водночас, кіберпростір настільки ускладнює процес притягнення до відповідальності суб’єктів, винних у вчиненні кіберзлочинів та завданні кібератак, що складно стверджувати про ефективність пристосування вже

існуючих контрольних та каральних механізмів до правовідносин, що виникають внаслідок порушення кібербезпеки, прав і свобод людини та громадянина у цій сфері.

З огляду на це, у тому числі, міжнародні організації активно працюють над питанням розробки заходів підвищення довіри у кіберпросторі. Наприклад, активізувалась діяльність ООН, спрямована на оцінку ролі заходів довіри в забезпеченні стабільності кіберпростору. З 2013 року ОБСЄ активно вдається до багатосторонніх заходів зміцнення довіри у сфері кібербезпеки та безпеки інформаційно-комунікаційних технологій. Іноді правові норми у цій сфері мають необов'язкову силу, а рекомендаційний характер, що свідчить про певний дипломатичний діалог у досягненні консенсусу з питання створення заходів довіри.

Через науково-технічний прогрес і впровадження нових інформаційно-комунікаційних технологій можливі загрози підривної діяльності, спрямовані проти фізичних і юридичних осіб, національних урядів, міжнародних організацій. При цьому дані технології дають змогу вчиняти зловмисні дії та іноді перебувати у відносній безпеці. Водночас проблемним аспектом цього питання, є процес встановлення особи, яка вчиняє зловмисні дії, а також причетність такої особи до наслідків вчиненого нею діяння. Мотиви підривної діяльності з використанням новітніх інформаційно-комунікаційних технологій досить різноманітні – від демонстрації своїх умінь та навичок всередині мережі, закінчуючи крадіжками інформації, грошових коштів або навіть здійснення дій, що мають за мету дестабілізувати діяльність у сфері інформаційних ресурсів та структур в рамках терористичного акту, кіберпростору, маніпулювання інформаційними ресурсами у всесвітній мережі. Звісно, такі дії можуть задовольняти потреби одних користувачів та порушувати права, свободи, інтереси інших, слугувати людству та стати небезпечним засобом впливу на суспільство, світову спільноту.

Отже, очевидний глобальний характер даної проблеми, що зумовлює потребу тісного співробітництва держав, міжнародних організацій, громадськості. На нашу думку, одним з

першочергових завдань на даному етапі має стати забезпечення не лише інтересів держав у сфері інформаційної безпеки, а у першу чергу, задоволення потреб усіх користувачів – приватного сектора, фізичних осіб, посадових осіб тощо. Конкретні зусилля, які можуть бути прийняті міжнародної спільнотою для зміцнення інформаційної безпеки на глобальному рівні, зокрема, включають: розробку глобальних стандартів поведінки у кіберпросторі, розширення можливостей міжнародної правової системи в боротьбі з кіберзлочинністю; розвиток і заохочення передового досвіду у сфері інформування щодо надзвичайних ситуацій, створення нормативно-правової бази, що стосується принципів поведінки у кіберпросторі, а також відповідальності за порушення встановлених правил. Це сприятиме забезпеченню надійного і безпечного кіберпростору.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Камінська Н.В. Міжнародна інформаційна безпека в умовах глобалізації та інтеграції. Міжнародне право: виклики сьогодення: матер. міжнар. науково-практ. інтернет-конфер. (Київ, 20 грудня 2016 р.). К.: КНТЕУ, 2016. С. 22-27.

2. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности / Управление по вопросам разоружения ГА ООН/ [Електронний ресурс]. – Режим доступу: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N13/371/68/PDF/ N1337168.pdf?OpenElement

3. Ткачук П.П., Шемчук В.В., Сальник Ю.П., Мацевко Т.М., Корольова О.В. Основи протидії інформаційно-психологічному впливові в особливий період. Навчально-методичний посібник. Л.: НАСВ, 2015. 189 с.

4. Ткачук П.П., Гула Р.В., Сивак О.І., Щурко О.М., Шемчук В.В. Інформаційна війна і національна безпека: монографія. Л.: НАСВ, 2015. 265 с.