УДК 343.3

Шемчук В.В.
Кваліфікаційно-дисциплінарна комісія прокурорів

ОСНОВНІ НАПРЯМИ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ КІБЕРБЕЗПЕКИ

У статті досліджуються основні засади й напрями міжнародного співробітництва України у сфері кібербезпеки. Виходячи з аналізу чинного національного законодавства, міжнародно-правових актів, міжнародної експертної діяльності, функціонування деяких міжнародних організацій, виокремлено пріоритети такого співробітництва з метою забезпечення ефективної системи кібербезпеки, міжнародної інформаційної безпеки загалом.

Ключові слова: *кібербезпека, кіберзагрози, міжнародне співробітництво, інформаційно-комунікаційні технології, інформаційна безпека.*

Постановка проблеми. Ураховуючи той факт, що з кінця XX – початку XXI століть відбуваються стрімкі процеси розвитку інформаційно-комунікаційних технологій, що поширюються практично на всі сфери життя, кардинально змінилися та продовжують змінюватися способи їх використання. Деякі з них сприяють задоволенню потреб людини, суспільства й держави, а деякі в незаконних, протиправних цілях підривають віру населення в здатність держави сприяти створенню та гарантуванню належного рівня безпеки серед громадян, що є однією з основних її функцій.

Ідеться про національну безпеку та міжнародну безпеку, що в умовах сучасності, звісно, не виключає інформаційну безпеку загалом і кібербезпеку зокрема. Це підтверджують наявні та потенційно можливі явища й чинники, що створюють небезпеку життєво важливим національним інтересам України в кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства й держави. Водночас агресія Російської Федерації й інші докорінні зміни в зовнішньому та внутрішньому безпековому середовищі України вимагають невідкладного створення національної системи кібербезпеки як складової частини системи забезпечення національної безпеки України [1].

Аналіз останніх досліджень і публікацій. Питанням феноменів інформаційної безпеки, кіберпростору в останні роки приділяли увагу як вітчизняні, так і зарубіжні дослідники. З-поміж них варто виокремити К. Бейкер, Р. Браста, І. Забару, О. Дзьобань, Н. Камінську, Дж. Карра, Д. Карпентера, О. Кирилюк, Дж. Кілуффо, Р. Кларка, М. МакКоннелла, П. Розенцвайга, М. Шмітта, А. Пазюка, В. Петрика, В. Пилипчука та ін. У своїх роботах вони переважно вивчають окремо питання інформації й інформаційної безпеки, міжнародної інформаційної безпеки, теорії інформаційного суспільства, а також окремо кіберзлочинності, кіберконфліктів тощо.

Постановка завдання. Мета статті полягає у виокремленні й аналізі основних засад і напрямів міжнародного співробітництва України у сфері кібербезпеки на основі вивчення чинного національного законодавства, міжнародно-правових актів, міжнародної експертної діяльності та роботи спеціально уповноважених інституцій у цій сфері.

Виклад основного матеріалу дослідження. На наше переконання, з огляду на наявну законодавчу основу та практику її реалізації, на доктринальні джерела, потребує уточнення розуміння понять «безпека», «інформаційна безпека», «кібербезпека». Найбільш різноманітними підходами до розуміння природи й сутності відзначається поняття «безпека». Зокрема, як підкреслює В. Ліпкан, ця категорія розглядається з-поміж іншого як гарантована конституцією, законодавством і практичними заходами захищеність і забезпеченість життєво важливих інтересів об'єкта від зовнішніх і внутрішніх загроз; як стан захищеності людини, суспільства й держави від зовнішніх і внутрішніх небезпек і загроз, який базується на діяльності людей, суспільства, держави, світового співтовариства щодо вивчення, виявлення, ідентифікації й

аутентифікації, попередження й усунення небезпек і загроз, мінімізації дії негативних наслідків, здатних унебезпечити фундаментальні цінності антропо-соціокультурного середовища, зашкодити стійкому розвитку системи безпеки; як стан управління небезпеками та загрозами, коли останні можуть відігравати конструктивну роль (синергетичний підхід); як органічна система організації державної влади щодо реалізації потреб та інтересів людини, фундаментальних засад існування будь-якої системи тощо [2, с. 42].

Загалом поняття «безпека» має комплексний характер, відзначається розгалуженою системою норм, що пронизують усі сфери життєдіяльності людства, передбачені й унормовані законом. Глобалізаційний характер трансформує класичне значення поняття безпеки в якісно нове, що пояснюється безпековою політикою держав, тобто в таке, що стосується всіх без винятку суб'єктів на міжнародно-правовій арені з огляду на виключну роль для останніх.

Важливе значення має з'ясування сутності поняття міжнародної колективної та національної безпеки. Так, колективну безпеку можна визначити як співробітництво держав із метою підтримання миру у світовому чи регіональному масштабах, міжнародну безпеку розглядають як стан міжнародних відносин, який виключає порушення та реальну загрозу розвитку людства, як діяльність держав і міжнародних інститутів щодо підтримання такого стану, універсальну систему механізмів, заходів і гарантій, які виключають застосування сили [3].

Переважно міжнародна безпека стосується процесів роззброєння та ядерної безпеки світу, однак Перший комітет ГА ООН порушив питання про досягнення у сфері інформатизації й телекомунікацій у контексті міжнародної безпеки. Заслуговує на увагу теза щодо віднесення інформаційної безпеки до системи міжнародної безпеки [4–5].

Водночас національна безпека визначається як стан захищеності життєво важливих інтересів особи, суспільства та держави. У сучасних умовах це невід'ємна властивість і водночас необхідна умова життєдіяльності та життєздатності особи, суспільства й держави. Згідно з п. 13 Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 2007 р. «інформаційна безпека визначається як стан захищеності життєво важливих інтересів людини, суспільства й держави, за якого запобігається нанесення шкоди через неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання й порушення цілісності, конфіденційності та доступності інформації» [6].

Залежно від об'єкта впливу інформаційну безпеку поділяють на такі види:

– інформаційну безпеку особи, яку розуміють як стан захищеності безпосередньо здоров'я людини в контексті наслідків негативного впливу інформації, коли остання може мати деструктивний вплив на сприйняття дійсності в результаті зловживань;

– інформаційну безпеку суспільства, що знаходить відображення переважно в конституційних положеннях. Так, ст. 17 Конституції України визначає інформаційну безпеку як одну з найважливіших функцій держав і покладає обов'язок її захисту на весь народ України; ч. 2 ст. 34 Конституції України зазначає: «Кожен має право вільно збирати, зберігати, використовувати й поширювати інформацію усно, письмово або в інший спосіб – на свій вибір» [7]. Ця норма узгоджується зі ст. 19 Міжнародного пакту про громадянські та політичні права ООН і конкретизується Конституційним Судом України в Рішенні від 20.01.2012 р. № 2-рп/2012;

– інформаційну безпеку держави, що розглядається з погляду наданої відповідним суб'єктам державної влади компетенції, необхідної для здійснення передбаченої законом діяльності. Зазначений вид безпеки кореспондується здебільшого з поняттям національної безпеки, котре відображене в абз. 2 ст. 1 Закону України «Про основи національної безпеки України» від 2003 р. й означає «захищеність життєво важливих інтересів людини й громадянина, суспільства й держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання й нейтралізація реальних і потенційних загроз національним інтересам у відповідних сферах» [8–9].

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» від 2017 р. визначено правові й організаційні основи забезпечення захисту життєво важливих інтересів людини й громадянина, суспільства та держави, національних інтересів України в кіберпросторі; основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб і громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Так, у цьому Законі кібербезпека трактується як захищеність життєво важливих інтересів людини й громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання й нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі [10].

Метою Стратегії кібербезпеки України 2016 р. є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства й держави. Забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини й громадянина, суспільства та держави в кіберпросторі досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів [1]. Згадана Стратегія базується на положеннях Конвенції про кіберзлочинність, ратифікованої 2005 р., законодавства України щодо основ національної безпеки, засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом і спрямована на реалізацію до 2020 р. Стратегії національної безпеки України, затвердженої Указом Президента України від 26.05.2015 р. № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України».

Основу національної системи кібербезпеки становитимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, на які мають бути покладені в установленому порядку визначені Стратегією завдання. Наприклад, на Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції покладено здійснення заходів із підготовки держави до відбиття воєнної агресії в кіберпросторі (до кібероборони); здійснення військової співпраці з НАТО, пов'язаної з безпекою кіберпростору та сумісним захистом від кіберзагроз; забезпечення у взаємодії з Державною службою спеціального зв'язку та захисту інформації України й Службою безпеки України кіберзахисту власної інформаційної інфраструктури [1].

Визначені на законодавчому рівні пріоритети та напрями забезпечення кібербезпеки України включають насамперед розвиток безпечного, стабільного й надійного кіберпростору, що має полягати зокрема у виробленні й оперативній адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягненні сумісності з відповідними стандартами ЄС і НАТО; у розвитку міжнародного співробітництва у сфері забезпечення кібербезпеки, підтримці міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, у поглибленні співпраці України з ЄС і НАТО задля посилення спроможностей України у сфері кібербезпеки, участі у заходах зі зміцнення довіри в кіберпросторі, які проводяться під егідою ОБСЄ тощо.

На підставі ст. 14 Закону 2017 р. регламентовано засади міжнародного співробітництва у сфері кібербезпеки за такими напрямами.

1. Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами й спеціальними службами, а також із міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю.

2. Україна відповідно до міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, може брати участь у спільних заходах із забезпечення кібербезпеки, зокрема в проведенні спільних навчань суб'єктів сектора безпеки й оборони в рамках заходів колективної оборони з дотриманням вимог законів України «Про порядок направлення підрозділів Збройних Сил України до інших держав» і «Про порядок допуску й умови перебування підрозділів збройних сил інших держав на території України».

3. Відповідно до законодавства України у сфері зовнішніх відносин суб'єкти забезпечення кібербезпеки в межах своїх повноважень можуть здійснювати міжнародну співпрацю у сфері кібербезпеки безпосередньо на двосторонній або багатосторонній основі.

4. Інформацію з питань, пов'язаних із боротьбою з міжнародною кіберзлочинністю, Україна надає іноземній державі на підставі запиту, додержуючись вимог законодавства України та її міжнародно-правових зобов'язань. Така інформація може бути надана без попереднього запиту іноземної держави, якщо це не перешкоджає проведенню досудового розслідування чи судового розгляду справи й може сприяти компетентним органам іноземної держави в припиненні кібератаки, своєчасному виявленні й припиненні кримінального правопорушення з використанням кіберпростору [10].

Для реалізації таких напрямів міжнародного співробітництва України у сфері кібербезпеки, на нашу думку, важливим є й вивчення відповідного зарубіжного досвіду, діяльності міжнародних організацій у згаданій сфері, прийнятих ними актів і ефективності їх реалізації.

Як відомо, перші здобутки у сфері інформатизації й телекомунікацій у контексті міжнародної безпеки з'являються в 1998 р., а їх дослідження є завданням Першого комітету Генеральної Асамблеї Організації Об'єднаних Націй. На думку останнього, забезпечити інформаційну безпеку можна лише в разі широкого міжнародного співробітництва, котре включає залучення держав, приватного сектора, а також громадянського суспільства до обговорення та вирішення нагальних проблем [11–12]. Тому було створено групу урядових експертів, діяльність яких пов'язана з аналізом досягнень із питань інформатизації та телекомунікацій, застосуванням інформаційно-комунікаційних технологій у контексті міжнародної безпеки. Перша робоча група проводила засідання у 2004–2005 рр., друга група – з 2009 р. до 2010 р., третя – з 2012 р. до 2013 р., четверта – з 2014 р. Серед результатів їхньої діяльності відзначимо Дослідження № 33, Досягнення у сфері інформатизації й телекомунікацій у контексті міжнародної безпеки, Доповідь у контексті обговорення питань інформаційної безпеки, Досягнення у сфері застосування інформаційно-комунікаційних технологій у контексті міжнародної безпеки й т. д.

Шляхом усебічного обміну думками стосовно досягнень у сфері застосування інформаційно-комунікаційних технологій у контексті безпеки міжнародні експерти, обрані на основі справедливого географічного розподілу, активно працювали над явними й можливими загрозами, а також над пошуком спільних взаємоузгоджених шляхів, спрямованих на їх усунення. На їхнє переконання, наявні та потенційні загрози у сфері інформаційної безпеки варто віднести до найбільш серйозних проблем XXI сторіччя. Це пояснюється тим, що у зв'язку з науково-технічним прогресом і впровадженням нових інформаційно-комунікаційних технологій загрози є похідними від широкого кола джерел і проявляються передусім у підривній діяльності, спрямованій проти фізичних і юридичних осіб, національної інфраструктури й урядів. Наслідки таких загроз тісно пов'язані з усіма сферами життя, котрі становлять глобальну систему міжнародної спільноти.

Групи урядових експертів наголошували на низці рекомендацій, зокрема на необхідності продовження діалогу між суб'єктами використання інформаційно-комунікаційних технологій, прийняття заходів щодо обміну думками та збільшення рівня довіри між зазначеними суб'єктами, здійснення обміну інформацією стосовно національних законів і стратегій, що можуть слугувати прикладом для інших країн; здійснення допомоги країнам, котрі стали на шлях розвитку в аспекті створення необхідного потенціалу для боротьби з кіберзлочинністю в цих країнах; створення загальної бази, спрямованої на уніфікацію норм із питань попередження й боротьби проти наявних і потенційних загроз у сфері використання інформаційно-комунікаційних технологій [11–13]. У підсумку вкрай важливо систематично проводити оцінку стану кібербезпеки, інформаційної безпеки всередині країн, їх регіонів, надавати рекомендації зі зміцнення рівня інформаційної безпеки на глобальному рівні.

Суттєвий прогрес у цій сфері спостерігається в деяких державах, проте очевидний і той факт, що чимало держав на цьому шляху значно відстають і гальмують ті чи інші напрями міжнародного співробітництва у сфері кіберпростору. Так, серед активних учасників такого діалогу слід відзначити Австралію, представники якої запевняли, що для максимального використання потенціалу всесвітньої мережі Інтернет потрібно створити надійний, безпечний і стійкий кіберпростір. Він має бути спрямований на задоволення не лише потреб держав, а на задоволення потреб усіх користувачів (приватного сектора, фізичних осіб, а також держав загалом). Федеративна Республіка Німеччина й собі прийняла Стратегію у сфері кібербезпеки 2011 р., сутність якої полягає в тому, що всі урядові органи, які займаються проблемами кібербезпеки, повинні тісно й напряму співпрацювати один з одним. Співпраця повинна бути налагоджена з приватним сектором у рамках центру кіберреагування з метою швидкого виявлення й аналізу великих інцидентів у сфері інформаційних технологій, а також із метою напрацювання рекомендацій, що стосуються вжиття заходів захисту [3, с. 13–15].

Держави – члени ООН акцентували й продовжують акцентувати увагу на необхідності налагодження стійкого діалогу між країнами та запровадження дієвих механізмів протидії викликам, якими супроводжується їх діяльність у кіберпросторі. Одними з пріоритетних напрямів покликані стати створення мирної, безпечної, стійкої й відкритої інформаційної сфери; відповідальна поведінка держав; заходи зміцнення довіри й обміну інформацією; заходи з нарощування потенціалу тощо. У результаті потребують розроблення гло-

бальні стандарти поведінки в кіберпросторі, розширення можливостей міжнародно-правової системи в попередженні й боротьбі з кіберзлочинністю; розвиток і заохочення позитивного досвіду у сфері інформування щодо надзвичайних ситуацій, створення стандартів поведінки в кіберпросторі.

Поряд із цим кожна держава, включаючи Україну, має створити ефективну національну систему кібербезпеки; посилювати спроможності суб'єктів сектора безпеки й оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом і кіберзлочинністю, поглиблювати міжнародне співробітництво в цій сфері. Слід підкреслити необхідність забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України, порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки й оборони України (критична інформаційна інфраструктура) тощо.

Конкретні зусилля мають бути спрямовані на забезпечення дієвих інструментів функціонування національної системи кібербезпеки, зміцнення інформаційної безпеки на національному, наднаціональному й міжнародному універсальному рівнях, ураховуючи глобальний вимір порушеної проблематики.

Висновки. Використання сучасних інформаційно-комунікаційних технологій, без сумніву, виходить за рамки національної безпеки, тому потребує застосування дієвих механізмів протидії загрозам у кіберпросторі. Будь-яка кібератака розпочинається з використання інформаційно-комунікаційних технологій, однак може дуже швидко вийти за межі віртуального світу, створюючи загрозу урядам, бізнес-середовищу й індивідам. Тому забезпечення кібербезпеки, інформаційної безпеки загалом є одним із пріоритетних напрямів діяльності не лише держав, а й їх регіональних об'єднань та всієї світової спільноти. Це той пріоритет, який фактично об'єднує людей різних континентів, держави, міжнародні організації тощо. Незважаючи на успішний досвід окремих держав, певні позитивні зрушення в напрямі міжнародної співпраці у сфері кібербезпеки на рівні ООН, НАТО, ЄС, ОБСЄ, важливо не зупинятися на досягнутих результатах, оскільки інформаційно-комунікаційні технології продовжують стрімко розвиватися, так само, як збільшується чисельність кіберзагроз і сфера їх поширення.

Таке міжнародне співробітництво у цій сфері повинне мати системний і послідовний характер, супроводжуватися ґрунтовними дослідженнями, особливо стосовно попередження й усунення загроз кібербезпеки, успішного зарубіжного досвіду в цій сфері.

Список літератури:

1. Про рішення Ради національної безпеки і оборони України від 27.01.2016 р. «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 р. № 96/2016

2. Безпека. Міжнародна поліцейська енциклопедія: у 10 т. / Відп. ред. Ю. Римаренко, Я. Кондратьєв, В. Тацій, Ю. Шемшученко. К.: Вид. Дім «Ін Юре», 2003. Т. 1: Теоретико-методологічні та концептуальні засади поліцейського права та поліцейської деонтології. С. 41–46.

3. Камінська Н., Чухно О. Пріоритети міжнародної співпраці у сфері забезпечення інформаційної безпеки Публічне право. 2015. № 4. С. 25–32.

4. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2012–2013. Управление по вопросам разоружения ГА ООН. URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N13/371/68/PDF/N1337168.pdf?OpenElement.

5. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция 56/19, принятая Генеральной Ассамблеей. По докладу Первого комитета (A/56/533).

6. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.: Закон України № 537-V від 09.01.2007 р. URL: http://zakon2.rada.gov.ua/laws/show/537-16.

7. Конституція України 1996 р. Відомості Верховної Ради України. 1996. № 30. С. 141.

8. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. Юридичний журнал. 2009. № 5. С. 122–134.

9. Про основи національної безпеки України: Закон України № 964-IV від 19.06.2003 р. URL: http://zakon3.rada.gov.ua/laws/show/964-15.

10. Про основні засади забезпечення кібербезпеки України. Закон України від 5.10.2017 р. № 2163-VIII. Відомості Верховної Ради. 2017. № 45. Ст. 403.

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

12. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция 65/41, принятая Генеральной Ассамблеей 8 декабря 2010 г. Доклад Первого комитета (A/65/405).

13. Камінська Н. 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.

14. Кирилюк О. Міжнародно-правові аспекти використання кіберпростору у військових цілях. Український часопис міжнародного права. 2014. Спецвипуск: Нові імена в науці міжнародного права. С. 80–86.

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

ОСНОВНЫЕ НАПРАВЛЕНИЯ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

В статье исследованы основания и направления международного сотрудничества Украины в области кибербезопасности. Исходя из анализа действующего национального законодательства, международно-правовых актов, международной экспертной деятельности, функционирования некоторых международных организаций выделены приоритеты такого сотрудничества с целью обеспечения эффективной системы кибербезопасности, международной информационной безопасности в целом.

Ключевые слова: *кибербезопасность, киберугрозы, международное сотрудничество, информационно-коммуникационные технологии, информационная безопасность.*

MAIN DIRECTIONS OF INTERNATIONAL COOPERATION IN THE FIELD OF CYBERSECURITY

The article examines the main principles and directions of international cooperation of Ukraine in the field of cybersecurity. Based on the analysis of current national legislation, international legal acts, international expert activities, the operation of some international organizations outlined the priorities of this cooperation with the objective of ensuring effective systems cybersecurity, international information security in general.

Key words: *cyber security, cyber threats, international cooperation, information and communication technologies, information security.*