Наталія Камінська,
доктор юридичних наук, професор,
професор кафедри гуманітарних та
загальноправових дисциплін
Національної академії внутрішніх справ

Олексій Чухно,
магістр права

УДК 341.23:004.735.5

Пріоритети міжнародної співпраці у сфері забезпечення інформаційної безпеки

Світ XXI сторіччя характеризується невпинним процесом розвитку усіх без винятку сфер життя, нівелювати значення інформації у процесі розвитку світу означає піддати під сумнів процес еволюції. Зазначене твердження пояснюється тим, що наразі жодна сфера суспільного життя не залишилася без впливу інформації, адже саме вона має визначальний вплив на сучасне інформаційне суспільство.

Сучасний світ повною мірою застосовує інформацію не лише як засіб комунікації, а й як спосіб задоволення інших потреб. Пропорційно зростаючий попит та пропозиція утворюють різні способи задоволення потреб. Однак з-поміж тих, що функціонують у правовій сфері є і такі, котрі покликані дестабілізувати розвиток у сферах задоволення потреб. Випадки використання інформації у незаконних, протиправних цілях підривають довіру громадян щодо здатності держави сприяти утворенню належного рівня безпеки серед громадян, що є однією з основних її функцій.

Метою статті є аналіз поняття інформаційної безпеки в контексті національного законодавства, міжна-

родно-правових актів, міжнародної експертної діяльності, а також дослідження сучасних досягнень протидії зловживань у сфері інформаційної безпеки в контексті науково-технічного прогресу.

Питанням феномену інформації та інформаційної безпеки останнім часом займається значна кількість дослідників, з яких варто виокремити В. Г. Пилипчук, О. П. Дзьобань, В. М. Петрик, А. В. Пазюк та ін. У своїх працях вони досліджують окремо питання інформації та інформаційної безпеки України, проте, без залучення міжнародного досвіду у цій сфері, практики зарубіжних країн.

Ключовим поняттям при дослідженні інформаційної безпеки є «інформація». Наразі, говорити про існування єдиного підходу щодо його дефініції не має можливості, адже, існує безліч точок зору щодо його визначення. Феномен інформації на основі історико-правових і філософських аспектів пояснюється таким чином, що при розгляді поняття «інформації» слід враховувати такі ключові аспекти:

– концептуальні засади розуміння суті інформації й теорії інформації, що містяться у дослідженнях і вживані в математиці, фізиці, кібернетиці не повністю відповідають значенню даного явища для суспільних відносин;

– поняття «інформація» не зовсім доречно впроваджувати і використовувати в контексті науково-технічних досліджень. Саме в цьому полягає одна з причин труднощів у визначенні значення цього терміну;

- у розумінні інформації та описанні її поняття мовна мотивація має не менш важливе значення, аніж аналіз характеристики, структури, природних властивостей і самого змісту цього феномена;

- не зовсім коректним видається зведення поняття «інформація» до слів «відомості», «дані», «сигнали», «команди» тощо, та відповідне його юридичне трактування в чинному законодавстві [1, с. 13].

Поряд з визначеннями, які надають науковці, доцільно зазначити законодавчо-закріплений підхід до розуміння дефініції. Так, відповідно до абз. 3 ч. 1 ст. 1 Закону України «Про інформацію» 1992 р. «інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [2]. Зауважимо, що це поняття регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації як і зазначено у преамбулі вищенаведеного Закону.

Широка сфера застосування поняття «інформація», що відображена в законодавчо закріпленому понятті, пояснюється особливим статусом інформації в суспільстві, у спробі законодавця врегулювати всі можливі сфери використання інформації. Слушною є думка В. Г. Пилипчука й О. П. Дзьобаня щодо виникнення проблем розуміння цього поняття через його ототожнення в усіх сферах суспільного життя без належної конкретизації [3, с. 12-14].

У контексті обраної теми, наступним поняттям, котре потребує належної конкретизації є поняття «безпеки». Існує велика кількість підходів до його розуміння, тож потрібно зупинитися на основних із них, а також відобразити внутрішню будову та значення поняття «безпека».

Так, на думку В. Ліпкана, «безпека» розглядається як:

1. гарантована конституцією, законодавством і практичними заходами захищеність і забезпеченість життєво важливих інтересів об'єкта від зовнішніх і внутрішніх загроз;

2. стан захищеності людини, суспільства і держави від зовнішньої і внутрішньої небезпек і загроз, який базується на діяльності людей, суспільства, держави, світового співтовариства щодо вивчення, виявлення, ідентифікації та аутентифікації, попередження та усунення небезпек та загроз, мінімізації дії негативних наслідків, здатних унебезпечити фун-

даментальні цінності антропосоціокультурного середовища, зашкодити стійкому розвитку системи безпеки;

3. стан управління небезпеками та загрозами, коли останні можуть відігравати конструктивну роль (синергетичний підхід);

4. органічна система організації державної влади щодо реалізації потреб та інтересів людини, фундаментальним основам існування будь-якої системи;

5. явище, яке тотожне гомеостазису системи, під яким розуміють тип динамічної рівноваги, що є характерним для складних систем, які саморегулюються, і полягає у підтриманні суттєво важливих для збереження системи параметрів у допустимих межах;

6. стан захищеності особи, суспільства, держави від внутрішніх та зовнішніх загроз, який базується на діяльності людей, суспільства і держави, світового співтовариства щодо виявлення (вивчення), попередження, послаблення, усунення (ліквідації) і відображення небезпеки та загрози, здатних згубити їх, позбавити фундаментальних матеріальних та духовних цінностей, нанести неприйнятну (недопустиму об'єктивно і суб'єктивно) шкоду, унеможливити шлях для виживання та розвитку [4, с. 42].

Враховуючи наведене доцільно зазначити, що поняття «безпека» має комплексний характер та характеризується розгалуженою системою норм, що пронизують усі сфери життєдіяльності людства, передбачені та унормовані законом. Наразі поняття «безпеки» набуло нового значення, ця теза пояснюється глобалізаційним характером безпекової політики держав, тобто таким, що стосується всіх без винятку суб'єктів на міжнародно-правовій арені через виняткову роль для останніх.

Особливе значення займають поняття колективної, міжнародної та національної безпеки. Так, «безпека колективна» – співробітництво держав з метою підтримання миру в світовому чи регіональному масштабах, «безпеку міжнародну» 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 [5-6].

В основному, міжнародна безпека стосується здебільшого процесів роззброєння та ядерної безпеки світу, проте Перший комітет ГА ООН порушив питання стосовно досягнень у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки. Заслуговує на увагу теза щодо віднесення інформаційної безпеки до системи міжнародної безпеки.

Залучення національної безпеки в аспекті дослідження обраної теми має визначальний характер, адже на рівні національного законодавства і відбуваються основні процеси, на які націлені держави під час формування як колективної так і міжнародної безпеки. У свою чергу, національна безпека визначається як стан захищеності життєво важливих інтересів особи, суспільства та держави. Її значення на сучасному рівні розвитку суспільства не варто недооцінювати, це невід'ємна властивість і водночас необхідна умова життєдіяльності та життєздатності особи, суспільства та держави.

Відповідно до абз. 2 п. 13 Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» 2007 р. «інформаційна безпека визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [7].

В залежності від об'єкту впливу, інформаційну безпеку поділяють на :

- інформаційну безпеку особи;
- інформаційну безпеку суспільства;
- інформаційну безпеку держави [8].

Інформаційну безпеку особи варто розуміти як стан захищеності безпосередньо здоров'я людини в контексті наслідків негативного впливу інформації, у тому випадку, коли остання може мати деструктивний вплив на сприйняття дійсності в результаті зловживань. Інформаційна безпека суспільства, знаходить своє відображення переважно в конституційних положеннях. Так, ст. 17 Конституції України, визначає інформаційну безпеку як одну з найважливіших функцій держав та покладає обов'язок її захисту на весь народ України; ч. 2 ст. 34 Конституції України зазначає, що «Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір» [9]. Зазначена норма узгоджується з п. 2 ст. 19 Міжнародного пакту про громадянські та політичні права ООН, а також деталізується Конституційним Судом України у рішення від 20.01.2012 № 2-рп/2012 [10].

Інформаційна безпека держави розглядається з точки зору наданих відповідним суб'єктам державної влади, необхідної для здійснення законом передбаченої діяльності, компетенції. Зазначений вид безпеки кореспондується здебільшого з поняттям національної безпеки, котре відображено у абз. 2 ст. 1 Закону України «Про основи національної безпеки України» 2003 р. та означає «захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у відповідних сферах» [11].

Важливим при цьому є й аналіз зарубіжного досвіду в контексті інформаційної безпеки, дослідження сучасних досягнень протидії зловживань у сфері інформаційної безпеки в контексті науково-технічного прогресу.

Відповідно до Резолюції Організації Об'єднаних Нації №56/19 поняття інформаційної безпеки здебільшого розуміється у двох вимірах: як цивільна, громадянська або суспільна сфера, а також як військова сфера. Міжнародна спільнота оцінюючи невпинний розвиток інформаційних технологій з одного боку наголошує, що вони сприяють забезпеченню оптимальної ефективності при їх міжнародному використанні, однак з іншого боку говорить, що такі технології також можуть бути потенційно використаними за для цілей, котрі не є сумісними з завданнями, що полягають у забезпеченні інформаційної стабільності та безпеки. Стурбованість міжнародної спільноти викликана розвитком інформаційно-комунікаційних технологій (далі - ІКТ). За допомогою останніх можуть здійснюватися деструктивні діяння. Проте, поряд з діями окремих суб'єктів через засоби масової інформації все більше розвивається думка, про створення таких технологій не лише окремими суб'єктами, а й з боку держав, зокрема, для ведення війни та розвідки у політичних цілях. Зростаюча напруга у суспільстві зумовлює потребу у міжнародній співпраці, з метою ефективного реагування на дії, метою яких є знищення основ міжнародної безпеки.

Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки знаходять своє відображення з 1998 року, його дослідженням займається Перший комітет Генеральної Асамблеї Організації Об'єднаних Націй. На думку останнього, забезпечити інформаційну безпеку можливо лише у разі широкого міжнародного співробітництва, котре включає залучення держав, приватний сектор, а також громадянського суспільства до обговорення та вирішення нагальних проблем [12].

Обговорення питань, що пов'язані із застосуванням ІКТ в контексті міжнародної безпеки – процес достатньо планомірний. Починаючи з 1998 року і до сьогодні, щорічно проводяться засідання присвячені даному питанню на рівні Генеральної Асамблеї ООН. З метою здійснення колективних дій задля ліквідації діяльності, обумовленої зловмисним використанням ІКТ, створено відповідну групу урядових експертів, діяльність яких пов'язана з аналізом досягнень в сфері інформатизації та телекомунікацій в контексті міжнародної безпеки. До цього часу були створені чотири групи урядових експертів.

Перша група проводила свої засідання в 2004 – 2005 роках. Однак, враховуючи, що на той час це був перший досвід створення такої робочої групи в контексті даної проблеми, особливих результатів так і не було досягнуто. Це обумовлено тим, що група так і не досягла консенсусу щодо підсумкової доповіді. Друга група існувала з 2009 по 2010 рік. На відміну від першої, друга група урядових експертів змогла узгодити свою доповідь та продемонструвала її у 2010 році. Результатом їхньої діяльності є Дослідження № 33 Досягнення в сфері інформатизації і телекомунікацій в контексті міжнародної безпеки. Третя група урядових експертів розпочала свою діяльність у 2012 році і завершила обговорення у 2013 році. Зазначена група підготувала доповідь в контексті обговорення питань інформаційної безпеки та продемонструвала її результати на шістдесят восьмій сесії Генеральної Асамблеї Організації Об'єднаних Націй. Наразі створена четверта група урядових експертів, діяльність якої розпочалась у 2014 р. і спрямована на демонстрацію результатів аналізу стану досягнень у сфері застосування ІКТ в контексті міжнародної безпеки.

На основі всебічного обміну думками з питань пов'язаних з досягненнями у сфері застосування ІКТ в контексті міжнародної безпеки, займалися діяльністю 15 експертів, обраних на основі справедливого географічного розподілу, що також полягав у співпраці й обговоренні наявних та потенційних загроз, а також спільних кроків з метою їх усунення. На думку групи експертів, 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 ІКТ, загрози є похідними від широкого кола джерел і проявляються, передусім, у підривній діяльності, спрямованій проти фізичних і юридичних осіб, національної інфраструктури та урядів. Наслідки таких загроз тісно пов'язані з усіма сферами життя, котрі становлять глобальну систему міжнародної спільноти [11-12].

Сучасний стан розвитку ІКТ дає змогу вчиняти зловмисні дії та перебувати у відносній безпеці. Проблемним аспектом цього питання, є процес встановлення особи, котра вчиняє зловмисні дії, а також причетність такої особи до наслідків вчиненого нею діяння. Мотиви підривної діяльності з використанням новітніх ІКТ досить різні. Починаючи з 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. Актуальність цієї проблеми зумовлена стрімким розвитком ІКТ, що в свою чергу відкриває нові можливості для маніпулювання інформаційними ресурсами, котрі покликані задовольняти потреби користувачів. Подвійна природа таких технологій проявляється у тому, що вони покликані слугувати людству та є небезпечним засобом впливу на суспільство. Варто зауважити, що не причини, а, безпосередньо, умови – є вихідним поняттям такої діяльності.

Враховуючи наведене, глобальний характер цієї проблеми зумовлює потребу у тісній співпраці суб'єктів міжнародної діяльності. В рамках цього, група урядових експертів 2009-2010 років наголошує на таких рекомендаціях: необхідність продовження діалогу між суб'єктами використання ІКТ; прийняття заходів щодо обміну думками та збільшенню рівня довіри між зазначеними суб'єктами; здійснення обміну інформацією стосовно національних законів та 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, котра націлена уніфікувати норми боротьби проти наявних та потенційних загроз у сфері використання ІКТ.

У рамках документів А/66/152, А/65/154, на підставі п. 3 Резолюції 65/41 ГА ООН державам-членам запропоновано провести оцінку стану інформаційної безпеки усередині країн, надати рекомендації зі зміцнення рівня інформаційної безпеки на глобальному рівні [13]. Активним учасником діалогу між державами виступає Австралія, представники якої стверджують, 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.

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.

Федеративна Республіка Німеччина 2011 р. прийняла стратегію в контексті кібербезпеки, сутність якої полягає у тому, що всі урядові органи, які займаються проблемами кібербезпеки, повинні тісно і напряму співпрацювати один з одним. Співпраця повинна бути налагоджена з приватним сектором в рамках центру кіберреагування з метою швидкого виявлення і аналізу великих інцидентів у сфері інформаційних технологій, а також з метою напрацювання рекомендацій, що стосуються вжиття заходів захисту.

Основним, на чому наголошують держави-члени ООН, – є налагодження стійкого діалогу між країнами та запровадження дієвих механізмів протидії викликам, котрим супроводжується діяльність у кіберпросторі. Документом А/68/98 надано відповідний перелік рекомендацій державам-членам щодо доопрацювання норм національного законодавства з метою зміцнення рівня співпраці в цілях створення мирної, безпечної, стійкої і відкритої інформаційної сфери; відносно відповідальної поведінки держав; заходів зміцнення довіри і обміну інформацією; заходів з нарощування потенціалу.

На фоні нарощування потенціалу інших держав, Україна робить успішні кроки на шляху забезпечення безпеки у сфері кіберпростору та інформаційної безпеки в цілому. Про це, зокрема, свідчить формування нового підрозділу Кіберполіції у зв'язку з проведенням реформ правоохоронних органів.

Використання інформації як засобу досягнення мети, що виходить за рамки міжнародної безпеки, потребує застосування дієвих механізмів протидії. По-перше, до шляхів боротьби у сфері кіберпростору, варто віднести, діалог з іншими державами в контексті прийняття рішень колективного характеру, котрі стосуються

забезпечення рівня захищеності суб'єктів ІКТ у сфері інформаційної безпеки. По-друге, здійснити уніфікацію та інтеграцію існуючих дієвих способів боротьби з усіма загрозами у чинне міжнародне та національне законодавство. По-третє, застосовувати ідеологію конвергенції як основу розбуди сучасної ефективної політики міжнародного значення, котра покликана не лише знайти прогалини, що дозволять усунути зловживання у сфері застосування інформаційно-комунікаційних технологій, а й дозволять діяти на випередження на основі поєднання успішного досвіду боротьби окремих країн. Досягнення інформаційної безпеки є одним з пріоритетних напрямів не лише держави, а й світу. Інформаційна захищеність суспільства в усіх сферах діяльності – ось чи не головна мета діяльності влади, міжурядових організацій та безпосередньо самих громадян.

Список використаних джерел

1. *Пазюк А. В.* Прогрессивное развитие и кодификация свободы информации в международном праве: исторический обзор и современные реалии / А. В. Пазюк // Український часопис міжнародного права. – 2012. – № 4. – С. 62–69.
2. *Про* інформацію : Закон України № 2657-XII від 02.10.1992 / [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua
3. *Дзьобань О. П.* Феномен інформації: історико-правові та філософські аспекти / О. П. Дзьобань, В. Г. Пилипчук / Інформація і право. – 2015. – № 1. – С. 5–14.
4. *Безпека* // Міжнародна поліцейська енциклопедія: у 10 т. / Відп. ред. Ю. І. Римаренко, Я. Ю. Кондратьєв, В. Я. Тацій, Ю. С. Шемшученко. – К.: Вид. Дім «Ін Юре», 2003. – Т. 1 : Теоретико-методологічні та концептуальні засади поліцейського права та поліцейської деонтології. – С. 41-46.
5. *Доклад* Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2012 – 2013 / 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
6. *Достижения* в сфере информатизации и телекоммуникаций в контексте международной безопасности : Резолюция 56/19, принятая Генеральной Ассамблеей / По докладу Первого комитета (A/56/533).
7. *Про* Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України № 537-V від 09.01.2007/ [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/537-16
8. *Петрик В.* Сутність інформаційної безпеки держави, суспільства та особи / В. Петрик // Юридичний журнал. – 2009. – № 5. – С. 122 – 134.
9. *Конституція* України: прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року // Відомості Верховної Ради України. – 1996. – № 30. – С. 141.
10. *Міжнародний* пакт про громадянські та політичні права від 16.12.1966 / [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/995_043
11. *Про* основи національної безпеки України: Закон України № 964-IV від 19.06.2003/ [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/964-15
12. *Доклад* Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2009 – 2010 / Управление по вопросам разоружения ГА ООН. – Нью-Йорк, 2012.

13. *Достижения* в сфере информатизации и телекоммуникаций в контексте международной безопасности : Резолюция 65/41, принятая Генеральной Ассамблеей 8 декабря 2010 года / По докладу Первого комитета (A/65/405).

Камінська Н. В., Чухно О. Пріоритети міжнародної співпраці у сфері забезпечення інформаційної безпеки

У статті аналізуються поняття безпеки, інформаційної безпеки, міжнародної безпеки. У залежності від об'єкту впливу виділяються різновиди інформаційної безпеки, інформаційно-комунікаційних технологій та пріоритетні напрями протидії зловживанням у сфері інформаційної безпеки, забезпечення безпеки кіберпростору. Основну увагу зосереджено на дослідженні діяльності груп урядових експертів Генеральної Асамблеї Організації Об'єднаних Націй з питань досягнень у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки.

Ключові слова: інформаційна безпека, кіберпростір, конвергенція, міжнародне право, національна безпека, колективна безпека, міжнародна безпека.

Каминская Н. В., Чухно А. Приоритеты международного сотрудничества в сфере обеспечения информационной безопасности

В статье анализируются понятия безопасности, информационной безопасности, международной безопасности. В зависимости от объекта влияния выделяют разновидности информационной безопасности, информационно-комуникационных технологий и приоритетные направления противодействию злоупотреблениям в сфере информационной безопасности, обеспечения безопасности киберпространства. Основное внимание сосредоточено на исследовании деятельности групп правительственных экспертов Генеральной Ассамблеи ООН по вопросам дострижений в сферв информатизации и телекомуникаций в контексте международной безопасности.

Ключові слова: информационная безопасность, киберпространство, конвергенция, международное право, национальная безопасность, коллективная безопасность, межнародная безопасность.

Kaminska N., Chukhno O. The priorities of the international cooperation in the field of information security

The article analyzes the concepts of «information», «security» and «information security». It is also providing the reader with the concepts of «national security», «collective security», «international security». Information security is divided according to the object of influence. It is basically focusing on the staged investigation of the activity of Group of Governmental Experts of the General Assembly of the United Nations on developments in the field of information and telecommunications in the context of international security. The recommendations and comments of foreign countries in the context of ensurance of cyberspace security are also highlighted in the article.

Key words: information security, cyberspace, convergence, international law, national security, collective security, international security.