УДК 342.9

Ігор Діордіца,
канд. юрид. наук, доцент, голова
Інституту адміністративного правосуддя
Глобальної організації союзницького лідерства

ПОНЯТТЯ І ЗМІСТ КІБЕРЗАГРОЗ НА СУЧАСНОМУ ЕТАПІ

У статті досліджено поняття і зміст кіберзагроз на сучасному етапі. Акцентовано увагу на тому, що на міжнародному й національному рівнях відсутнє визначення поняття «кіберзагрози», і це має негативні наслідки. Запропоновано авторське розуміння терміна: «кіберзагрози» – протиправні карні дії суб'єктів інформаційних правовідносин, які створюють небезпеку життєво важливим інтересам людини, суспільства та держави загалом, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, а також відносинам щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації. Зазначено, що сутність кіберзагроз становлять їх суб'єкти, тобто суб'єкти інформаційних правовідносин, а об'єктом є безпосередньо інформація. Інформаційні інтервенції становлять суттєву загрозу кібернетичній безпеці. Зауважено, що загрози можуть бути як внутрішні, так і зовнішні. Для розроблення дієвого механізму протидії кіберзагрозам Україні запропоновано взяти за приклад наявну практику зарубіжних країн і міжнародної спільноти, привести її у відповідність до українських реалій.

Ключові слова: кібербезпека, інформаційна інтервенція, кіберзагроза, хактивісти, кібератресія, інформація, кіберпростір.

Постановка проблеми. Формування й ефективна реалізація кібербезпекової політики, в рамках якої розробляється комплекс заходів щодо прогнозування та протидії кіберзагрозам, є необхідною умовою розвитку суспільства знань. В умовах глобалізації інформаційних процесів, їх інтеграції в різні сфери суспільного життя керівництво провідних держав світу приділяє посилену увагу створенню й удосконаленню ефективних систем захисту критичної інфраструктури від зовнішніх і внутрішніх загроз кібернетичного характеру.

Відзначимо, що в багатьох провідних країнах світу вже сформовані загальнодержавні системи кібернетичної безпеки як найбільш оптимальні організаційні структури, що здатні в короткий проміжок часу акумулювати сили та засоби компетентних органів державної влади із залученням громадських для протидії кіберзагрозам.

В Україні також відбувається процес формування системи кібернетичної безпеки. Як складник такої системи варто розглядати єдину загальнодержавну систему протидії кіберзлочинності, пропозиції щодо створення якої ще у 2011 році доручалося розробити Кабінету Міністрів України за участю Служби безпеки України.

На загал інституційний ландшафт кібербезпеки можна позначити через організаційно-структурні й нормативно-правові зміни.

До структурних змін належить створення Міністерства інформаційної політики України, у складі Національної поліції – кіберполіції, Національного координаційного центру кібербезпеки, Ради з питань комунікацій – консультативно-дорадчого органу Кабінету Міністрів України, Об'єднаного інформаційно-аналітичного центру «Єдина Країна», Єдиного прес-центру з висвітлення АТО на базі Служби безпеки України тощо.

До нормативно-правових змін належить ухвалення оновленої Стратегії національної безпеки України [1], започаткування Партнерства у сфері стратегічних комунікацій між РНБО України та Міжнародним секретаріатом НАТО, які включають сферу кібербезпеки [2], ухвалення Стратегії кібербезпеки України [3].

Водночас недосконалість національного законодавства у сфері забезпечення кібернетичної безпеки значно підвищує ймовірність реалізації таких загроз, що негативно впливає на загальний рівень національної безпеки України [4]. Ці та інші фактори й зумовлюють актуальність теми дослідження.

Деякі аспекти проблемки кібернетичної безпеки та кібернетичних загроз у той чи інший спосіб досліджувались у наукових працях таких вітчизняних учених, як наукова школа В.А. Ліпкана [5–19], І.В. Арістова [20–21], В.С. Цимбалюк [22–25], І.В. Сопілко [26] та інші, проте питання правового регулювання кібербезпеки, зокрема формування ефективного механізму правового регулювання протидії загрозам у кібернетичній сфері, на сучасному етапі є абсолютно новим, що зумовлює потребу в його ґрунтовному дослідженні.

Особливо варто зупинитись на тих загрозах, які існують у зв'язку з нині триваючою інформаційною війною в Україні та виявами кібертероризму, діяльністю хактивістів у світі. Окремо зазначимо праці таких науковців, як В.В. Куцаєв, Є.О. Живило, С.П. Срібний, Ю.О. Черниш, Д.С. Мінін, В.П. Шеломенцев, Д.С. Бірюков, С.І. Кондратов.

Метою статті є визначення поняття і змісту кіберзагроз на сучасному етапі.

Для досягнення поставленої мети, сформульовано завдання – здійснити етимологічний аналіз понять, які становлять основу категорійного ряду дослідження, а саме: інформаційний, загроза, кібернетичний і безпека, критична інфраструктура, інформаційні інтервенції, а потім шляхом їх поєднання й реалізувати мету наукового доробку.

Виклад основного матеріалу. Кіберзагрози в сучасному суспільстві набирають значного масштабу. Відтепер успішна атака хакерів може знеструмити область або країну, призвести до пограбування банку чи знищити успішну організацію. Наприклад, за різними оцінками, за 2015 рік із рахунків підприємств України зникло близько 100 млн грн. [27].

З метою проведення коректних та ефективних заходів щодо відвернення кіберзагроз і ліквідації їх негативних наслідків, передусім необхідною є їх легітимація – вироблення та закріплення законодавчої дефініції задля уникнення порізненості під час застосування цієї категорії, а також колізії з іншими нормативно-правовими актами, визначення їх змісту, уніфікованості правозастосовної практики.

Зауважимо, що, незважаючи на досить часте використання категорії «кібернетичні загрози» в доктрині, публіцистиці та повсякденному житті [28], її законодавче уніфіковане визначення поняття відсутнє як на національному, так і на міжнародному рівнях. Це відбувається на тлі того, що кіберзагрози за своєю природою не є локальними, тобто обмеженими певної територією або навіть державними кордонами, а, навпаки, вони становлять глобальне явище, яке має негативний і почасти деструктивний характер.

Для досягнення мети статті спочатку проаналізуємо наявні дефініції та, здійснивши їх ґрунтовний аналіз, запропоную авторське розуміння поняття «кіберзагрози».

Кібернетична загроза (кіберзагроза) – наявні й потенційно можливі явища та чинники, що створюють небезпеку інтересам людини, суспільства й держави через порушення доступності, повноти, цілісності, достовірності, автентичності режиму доступу до інформації, яка циркулює в критичних об'єктах національної інформаційної інфраструктури [29].

Цю дефініцію, на нашу думку, варто доповнити правомочностями, які закріплені в Законі України «Про інформацію» як основоположному в інформаційній сфері, в якій мають місце кіберзагрози, а саме: створення небезпеки загроз відносинам щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

Також не зовсім доречним є використання таких термінів, як *«явища»* й *«чинники»*.

Використовуючи тлумачний словник української мови, зазначимо, що «явище» – будь-який вияв змін, реакцій, перетворень тощо, які відбуваються в навколишньому природному середовищі; подія, факт [30]. «Чинник» – умова, рушійна сила, причина будь-якого процесу, що визначає його характер або одну з основних рис; фактор.

Зауважимо на тому, що загроза не може бути фактом або подією, у будь-якому випадку це дії. Аргументи щодо цього твердження наведемо дещо нижче по ходу виконання дослідження.

Щодо визначення терміна «кіберзагрози» як причини також це є некоректним, оскільки «загроза» – груба, зухвала обіцянка заподіяти яке-небудь зло (активна дія), неприємність; погрожування, нахваляння; можливість або неминучість виникнення чогось небезпечного, прикрого, тяжкого для кого-, чого-небудь; те, що може заподіювати яке-небудь зло, якусь неприємність [30, с. 268].

Саме останнім значенням цього денотату ми й будемо послуговуватись. Ще однією «невідомою» категорією в цій дефініції є «критичні об'єкти національної інформаційної інфраструктури», оскільки тлумачення одного невідомого й неуніфікованого терміна через використання такого ж іншого є неприпустимим і видається нелогічним.

Розглянемо таке визначення поняття кіберзагрози.

Кібернетичні загрози (кіберзагрози) – наявні й/або потенційно можливі явища та чинники, що створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства й держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [31].

Ця дефініція також потребує низки уточнень, а саме: що становить життєво важливі інтереси людини та громадянина? Чи є нагальною потреба закріплення саме формулювання «людина та громадянин»? Як саме визначити належність функціонування вищезазначених систем? Як співвідноситься це визначення й Законом України «Про основи національної безпеки України», і Стратегією національної безпеки України тощо.

«Кібернетичний» – той, що стосується до кібернетики.

Отже, ґрунтуючись на цих дефініціях, пропонуємо авторське розуміння: *«кіберзагрози»* – протиправні, карані дії суб'єктів інформаційних правовідносин, які створюють небезпеку життєво важливим інтересам людини, суспільства та держави загалом, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, а також відносинам щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

Базуючись на цьому визначенні, зауважимо, що зміст, тобто сутність, кіберзагроз становлять їх суб'єкти, тобто суб'єкти інформаційних правовідносин, а об'єктом є безпосередньо інформація.

У Доктрині інформаційної безпеки України (втратила чинність) було зазначено, що в інформаційній сфері України вирізняються такі життєво важливі інтереси:

1) *особи:* забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; недопущення несанкціонованого втручання в зміст, процеси оброблення, передачі й використання персональних даних; захищеність від негативного інформаційно-психологічного впливу;

2) *суспільства:* збереження та примноження духовних, культурних і моральних цінностей Українського народу; забезпечення суспільно-політичної стабільності, міжетнічної та міжконфесійної злагоди; формування й розвиток демократичних інститутів громадянського суспільства;

3) *держави:* недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав і міжнародних структур; ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригування державної політики в інформаційній сфері; побудова й розвиток інформаційного суспільства; забезпечення економічного та науково-технологічного розвитку України; формування позитивного іміджу України; інтеграція України у світовий інформаційний простір [32].

Під час визначення термінів пропонується надавати їх у більш широкому розумінні, враховуючи вже наявні напрацювання в таких галузях науки, як кібернетика, інформатика, інформаціологія, безпекознавство, кримінальне й інформаційне право тощо.

Обговорювання та розширення термінології щодо кіберпростору дасть змогу суспільству більш якісно й безпечно планувати свої дії в сучасному кіберпросторі. Додаткові терміни зроблять можливим лаконічно пояснити, що людська (суспільна) думка – це є аналоговий кібербіопростір, який за допомогою технічних засобів перетікає в технічний кіберпростір, там накопичується, багаторазово копіюється, обробляється та перетікає назад і аналоговий кібербіопростір у новому більш розвинутому й перевіреному всім суспільством вигляді, але вже для масового використання та розвитку суспільства на новому вищому рівні [31].

У міжнародному законодавстві й досі відсутнє єдине визначення понять: «кібернетична безпека», «кібернетична загроза», «кібернетичний захист», «кібернетичний простір», «кібернетична злочинність». Проблема кібербезпеки специфічна та глобальна, тому максимальна ефективність у боротьбі з новими загрозами може бути забезпечена, якщо міжнародні актори, приватні корпорації й асоціації об'єднають свої зусилля. Актуальність визначення змісту понять «кібербезпека» та «кіберзагроза» (авт.) є важливим моментом для покращення ефективності взаємодії на міжнародному рівні [33].

Кібернетичні загрози являють собою загрози, реалізація яких пов'язана з використанням відповідних ресурсів інформаційно-телекомунікаційних систем. Уразливими для реалізації кібернетичних загроз є об'єкти, функціонування комп'ютерних систем яких пов'язане з використанням ресурсів кіберпростору. Тобто об'єкти, завдання шкоди яким можливе шляхом деструктивного кібернетичного впливу (кібернетичної атаки) – інформаційного впливу з використанням кіберресурсів, спрямованого на уразливості комп'ютерних систем таких об'єктів. До об'єктів національної критичної інфраструктури, що потребують захисту від кібератак, необхідно зарахувати об'єкти, реалізація кібернетичних загроз щодо яких може призвести до настання таких наслідків, як надзвичайна ситуація; блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення й об'єктів підвищеної небезпеки; блокування роботи державних органів; блокування діяльності органів військового управління, Збройних Сил України загалом або втручання в автоматизовані системи керування зброєю; порушення безпечного функціонування банківської або фінансової системи держави; розголошення державної таємниці; масові заворушення [4]. Тобто кіберзагрози не можна обмежувати якоюсь однією сферою, частіше за все настання певних наслідків може спричинити інші, тобто ланцюгова реакція.

Унаслідок неналежного правового регулювання в національному кібернетичному просторі України спостерігається низка негативних явищ, які створюють реальні та потенційні загрози кібернетичній безпеці. У 2014 році на території Автономної Республіки Крим і південно-східних регіонах України здійснювався інформаційно-психологічний тиск на населення України з боку засобів масової інформації Російської Федерації, спостерігалася інформаційна експансія (чи інтервенція) в національний інформаційний простір України, захоплювались стратегічні об'єкти української телекомунікаційної інфраструктури.

Поділяємо наукову позицію, що з метою запобігання зловживанню інформацією та для захисту інформаційних прав сучасний стан забезпечення національної й кібернетичної безпеки України потребує розроблення науково обґрунтованої державної політики в цій галузі, визначення системи національних цінностей, життєво важливих інтересів особистості, суспільства та держави, визначення зовнішніх і внутрішніх загроз цим інтересам, пошуку ефективних заходів для забезпечення безпеки в усіх її сферах, захисту від інформаційних загроз і реалізації права на отримання достовірної інформації (права на доступ до інформації [34]). Паралельно все вищевикладене свідчить про потребу прийняття нормативно-правових актів, у яких був би передбачений механізм захисту інформаційних прав від протиправних дій третіх осіб щодо інформації. Більше того, ухвалена Стратегія кібербезпеки за своїм змістом у концептуальному плані не відповідає змісту саме стратегії: вона не передбачає досягнення стратегічних цілей, немає стратегічного рівня управління й відповідних категорій, не оперує стратегічним інструментарієм: стратегічне планування, стратегічне прогнозування тощо. Відтак пропоновані якісні зміни мають тимчасовий, максимум тактичний характер, оскільки в рамках цієї

стратегії неможливо досягти стратегічних переваг і сформувати стратегічний баланс інтересів міжнародних організацій і транснаціональних корпорацій і національних інтересів України в кібернетичній сфері.

Розвиваючи далі ідею загроз у сфері кібербезпеки, зауважимо, що існує залежність країни й в інформаційному, і смисловому вимірах. Це відбувається тоді, коли країні не вистачає власних новин чи власних фільмів, і вона заповнює ці прогалини чужим продуктом. Україна є чітким прикладом цієї ситуації [35]. Так само можемо зазначити, що і Європа виявилася нездатною протистояти навалі інформаційного бруду з Росії, сформувати ефективну систему інформаційної політики, включаючи механізми нейтралізації дезінформаційних потоків із Росії.

Нашу думку підтверджують у дослідженні й фахівці НІСД [28, с. 107], зазначаючи, що не лише Україна, а і Європа та світ загалом виявилися не готовими до дій Росії, що заперечують будь-які встановлені міжнародні правила поведінки держави. Неготовність охоплює весь спектр існування західної цивілізації: від свідомості пересічних громадян [36] до політичних процесів і процедур, необхідність дотримання яких використовується Росією для досягнення її зовнішньополітичних цілей.

Інформаційні інтервенції становлять суттєву загрозу кібернетичній безпеці, оскільки остання є частиною національної безпеки, може завдавати шкоди як державі загалом, так і окремим фізичним особам. Створення дієвої системи забезпечення кібернетичної безпеки вимагає від державних органів України чіткого визначення правових засад державної політики в цій сфері та своєчасного реагування на динамічні зміни, що відбуваються у світі у сфері забезпечення кібернетичної безпеки з можливістю застосування міжнародного досвіду.

При цьому вибір конкретних засобів і способів забезпечення кібернетичної безпеки України зумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру й масштабам реальних і потенційних кібернетичних загроз життєво важливим інтересам людини та громадянина, суспільства й держави [35].

Нині виокремлюють такі *загрози кібербезпеці й безпеці інформаційних ресурсів:* уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична та моральна застарілість системи охорони державної таємниці й інших видів інформації з обмеженим доступом [37].

Знову акцентуємо увагу на постійному використанні законодавцями терміна *«критична інфраструктура»* за відсутності його легітимації в Україні.

Уперше в офіційних документах термін «критична інфраструктура» з'явився у 2006 р. в тексті Рекомендацій парламентських слухань з питання розвитку інформаційного суспільства, на жаль, без подальшого розвитку. У Стратегії національної безпеки «Україна у світі, що змінюється» (2012 р.) цей термін згадувався під час визначення шляхів зміцнення енергетичної безпеки та напрямів забезпечення інформаційної безпеки. У новій Стратегії національної безпеки України (2015 р.) термін «критична інфраструктура» використовується більш деталізовано. Уперше з-поміж «актуальних загроз національній безпеці» виокремлюються загрози критичній інфраструктурі, крім того, окремо в підрозділі «Загрози кібербезпеці і безпеці інформаційних ресурсів» згадується вразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак. Також уперше з-поміж «основних напрямів державної політики у сфері національної безпеки» названо забезпечення безпеки критичної інфраструктури та визначено пріоритети такого напряму. Відсутність визначення терміна «критична інфраструктура» в українському законодавстві і, як наслідок, відсутність переліку об'єктів, які потрібно зарахувати до неї, неодноразово створювали перешкоду для ефективного виконання першочергових безпекових завдань і відверненя кіберзагроз (*авт.*).

Критична інфраструктура України – це системи та ресурси, фізичні чи віртуальні, що забезпечують функції й послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки [38, с. 14–15].

Україна має швидко, надійно й ефективно реагувати на будь-які кіберзагрози, що неможливо без інтегрування та чіткої взаємодії всіх наявних ресурсів суб'єктів кібербезпеки. На засіданні Національного центру кібербезпеки розглянуто заходи щодо вдосконалення системи зберігання, передачі та оброблення даних державних реєстрів і баз даних із застосуванням сучасних інформаційно-комунікаційних технологій.

Окрему увагу приділено розбудові інтегрованої захищеної системи державних реєстрів, баз даних і дата-центрів для оброблення та резервного збереження інформації й відомостей державних електронних інформаційних ресурсів. Підготовка відповідних фахівців для державних суб'єктів забезпечення кібербезпеки визначена актуальним питанням, і така підготовка повинна відбуватись як в Україні, так і за її межами «відповідно до актуальних завдань, що стоять перед державою на цьому важливому напрямі» [39].

Аналіз законодавства у сфері кібербезпеки, а також організаційних заходів, спрямованих на розбудову ефективних систем кіберзахисту провідних країн світу, свідчить, що ключові світові гравці вдосконалюють власні можливості з кіберзахисту відповідно до трансформації сучасних кіберзагроз.

Останнім часом фіксується суттєва зміна форм, суб'єктів і наслідків реалізації основних загроз кібербезпеці держав. Так, кібератаки стають усе більш комплексними та складними, їх наслідки становлять загрозу ключовим національним інтересам, а їх організаторами або замовниками все частіше виявляються спецслужби іноземних держав чи терористичні організації.

Потреба реалізації ефективних заходів із протидії сучасним кібернетичним загрозам на національному рівні призводить до збільшення ролі в системах кібербезпеки країн спеціальних служб і правоохоронних органів, що мають контррозвідувальні функції й виконують завдання з протидії протиправній діяльності спецслужб іноземних держав і тероризму.

Аналізуючи системи кібербезпеки провідних країн світу, можна висновувати, що нині не існує уніфікованої моделі побудови національної кібербезпекової системи. Водночас важливим питанням залишається створення належної нормативно-правової основи для подальшої розбудови ефективних кіберспроможностей, закладення ключових підвалин національної кібербезпеки.

Так, натепер понад 50 країн світу мають стратегії кібербезпеки (в Україні подібною є Стратегія національної безпеки – авт.), які визначають ключові поняття кібербезпекової сфери, кіберзагрози, основні принципи побудови безпечного кіберпростору, напрями реалізації державної політики у сфері кібербезпеки, наголошують на важливій ролі державно-приватного партнерства та міжнародного співробітництва у сфері забезпечення кібербезпеки.

Поділяємо позицію, що одним із ключових питань організації ефективної роботи національних систем кібербезпеки залишається налагодження взаємодії між компетентними державними органами, які є суб'єктами кібернетичної безпеки, і здійснення координації з такої діяльності [40, с. 76].

Щодо зарубіжної практики протидії кіберзагрозам, зауважимо таке.

Наприклад, канадська стратегія кібербезпеки базується на тому, що метою забезпечення найсучаснішого використання кіберпростору, який є стратегічним активом, є прогнозування і протистояння кіберзагрозам, що виникають. У стратегії кібербезпеки Канади немає чіткого визначення дефініції «кібербезпека». Проаналізувавши цей документ, можна розуміти кібербезпеку як захист кіберсистем від шкідливого неправильного використання й інших деструктивних атак. Автори стратегії приділяють уваги визначенню кібератаки, підкреслюючи, що кібербезпека є засобом захисту від цих загроз [41].

Натепер ключова роль у забезпеченні кібербезпеки Сполучених Штатів Америки належить Міністерству внутрішньої безпеки (МВБ), яке було створене в результаті повного реформування спеціальних служб і силових відомств США після подій 11 вересня 2001 року, що поставили на перший план питання національної безпеки держави та захист її критичної інфраструктури. Відповідно до прийнятого 25 листопада 2002 року комплексного нормативно-правового акта у сфері безпеки – закону США «Про внутрішню безпеку» (Homeland Security Act of 2002), урядові структури, які займались забезпеченням комп'ютерної безпеки, перейшли під контроль цього новоствореного відомства. Указаний закон також посилив відповідальність за комп'ютерні злочини (включаючи довічне ув'язнення), зобов'язав інтернет-провайдерів надавати інформацію про клієнтів за вимогою правоохоронних органів, розширив права останніх щодо можливості перехоплення інформації (прослуховування телефонних переговорів і перлюстрацію електронних повідомлень) без дозволу суду, визначив основні напрями діяльності федеральних органів із підвищення ефективності захисту критичної інфраструктури США від кібератак, у тому числі об'єктів стратегічного значення, що перебувають у приватній власності [40].

Щодо запозичень, які варто було б використати, так це, на нашу думку, посилення відповідальності за комп'ютерні злочини й зобов'язання інтернет-провайдерів надавати інформацію про клієнтів за вимогою правоохоронних органів.

Значним досягненням у сфері забезпечення кібербезпеки є проведення відповідних конференцій. Уперше саміт із кібербезпеки – Cyber Security Summit – у рамках Мюнхенської безпекової конференції проведено не в Німеччині. Обговорення актуальних проблем кіберпростору відбулося в Кремнієвій долині – це дуже інноваційний організатор у всіх галузях кібербезпеки. Саме із цього регіону походять нові методи. Крім того, це міжнародне місце зустрічі [42].

Серед тем дискусії – протидія кібератакам, майбутнє ведення війн, розвиток норм і правил для кіберпростору, боротьба проти кібертероризму, а також економічне значення кібербезпеки [42].

Окремо варто зупинитися на реальних кіберзагрозах, які мали місце в Україні та світі.

Наприклад, міжнародна платіжна система SWIFT попередила про зростання кіберзагрози для банків, оскільки хакери знайшли нові способи проведення атак (13 грудня 2016 р.) [43].

А от американські сенатори, які обіймають високі посади у верхній палаті Конгресу США, – республіканці Джон Маккейн, Ліндсі Грем – і демократи – Чарльз Шумер і Джек Рід – оприлюднили спільне звернення щодо необхідності вивчити повною мірою кіберзагрозу з боку Росії [44]. Більше того, в березні минулого року в Сенат США подано законопроект щодо протидії дезінформації та пропаганді [45].

Чільні представники спецслужб США заявили на слуханні в Конгресі, що Росія становить значну кіберзагрозу для військової, дипломатичної, торговельної й життєво важливої інфраструктури США [46]. Росія є повномасштабним актором у кіберпросторі, який створює головну загрозу уряду США, військовій, дипломатичній, комерційній, іншій критично важливій інфраструктурі та ключовим мережам постачання послуг через її високорозвинену наступальну кіберпрограму, застосування складних тактик, техніки і процедур [47].

Німецьке Федеральне управління з інформаційної безпеки повідомило парламентським партіям і фракціям у Бундестазі, а також окремим політикам про нещодавні атаки на їхні сервери й попередило про можливість повторення подібних атак. Джерелом нападів найрізноманітніші відомства Німеччини, включаючи розвідку, вважають хакерів, які діють за

завданнями російських спецслужб. Висловлюється припущення про небезпеку маніпуляцій засобами шпигунства, дезінформації, кібератак і поширення неправдивих новин щодо результатів голосування на майбутніх виборах восени 2017 року до парламенту ФРН [48].

Європарламент ухвалив резолюцію щодо протидії російським ЗМІ. Резолюція має назву «Стратегічні комунікації ЄС як протидія пропаганді третіх сторін». У документі йдеться, що пропаганда є частиною «гібридної війни», спрямована на те, щоб «спотворити правду, посіяти сумніви й ворожнечу між країнами Союзу». У документі, зокрема, стверджується, що Росія надає фінансову підтримку опозиційним партіям та організаціям у країнах-членах ЄС, а також «використовує фактор двосторонніх міждержавних відносин для роз'єднання членів спільноти». Основні інформаційні загрози Євросоюзу – це агентство Sputnik, телеканал RT, фонд «Русский мир» і підвідомче російському МЗС федеральне агентство «Росструдничество».

Серед інших джерел пропаганди, яким, згідно з резолюцією, має протистояти Євросоюз, називаються угруповання «Аль-Каїда» та «Ісламська держава» [49].

Президент України Петро Порошенко закликав світ протидіяти російській кіберзагрозі, спонукав США «бути великими знову», продемонструвавши лідерство в питанні глобальної безпеки [50].

В Україні розпочато створення Центру оперативного реагування на загрози у сфері кібернетичної безпеки, допомогу якому надає уряд США. Здійснюються заходи щодо впровадження в діяльність Міноборони та ЗСУ засобів із захисту інформації в інформаційно-телекомунікаційних системах з урахуванням стандартів провідних країн світу. Також розроблено проект Стратегії кібероборони України, який уже погоджений із представниками європейського командування Збройних сил США, Агенції з національної безпеки Чеської Республіки. Наразі цей документ знаходиться на розгляді профільного комітету Верховної Ради та апарату РНБО [51].

На жаль, широкого обговорення цей Законопроект не має, до його розроблення не залучені представники недержавних організацій, юристи, представники Національної академії правових наук, наукові школи з інформаційного права та інформаційної політики. Тому говорити про необхідність цього документи як окремого немає підстав. Виникає багато запитань передусім у необхідності цього документа за умови вже наявних: Стратегії національної безпеки України, Стратегії кібербезпеки, Закону України «Про основи національної безпеки України» тощо. Оскільки в нас немає змогу аналізувати конкретний текст документа, цю дискусію винесемо за межі статті.

Національний банк України та Незалежна асоціація банків України планують створити спільний центр реагування альянсу в банківській системі. Керівництвом НБУ презентовано проект створення «Центру реагування на інциденти кібернетичної безпеки у банківській системі та платіжному просторі України CERT-NBU». Відповідно до своєї головної мети створення, CERT-NBU має допомогти у вирішенні проблем боротьби з кіберзагрозами, буде сприяти розвитку банківської системи України загалом [52].

Також акцентуємо увагу на тому, що кібербезпека не може регулюватися лише на національному або європейському рівнях, для цього необхідні глобальні зв'язки.

У питаннях протидії кіберзагрозам повинні застосовуватися принципово нові механізми. Ефективним засобом протидії кіберзагрозам може стати розбудова нових ліній оборони, однією з яких має стати міжнародне співробітництво між усіма зацікавленими акторами, щоб у разі кібератаки компетентні органи сторони, яка зазнала нападу, і сторони, з території якої походить кібератака, оперували механізмами оперативного сповіщення про такий інцидент, а також спільної боротьби з ним.

Саме тому надзвичайно важливо якомога швидше консолідувати зусилля держав для запобігання новітнім кіберзагрозам, й одним із основних напрямів є зміцнення політичної довіри між урядами.

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

Вітчизняні реалії кібербезпекової сфери свідчать про низку важливих проблем, що заважають створити ефективно діючу систему протидії загрозам у кіберпросторі. До таких проблем передусім належать термінологічна невизначеність, відсутність належної координації діяльності відповідних відомств, залежність України від програмних і технічних продуктів іноземного виробництва, складнощі з кадровим наповненням відповідних структурних підрозділів.

Активну позицію щодо протидії кіберзагрозам займає й провідна міжнародна безпекова організація – НАТО (Cooperative Cyber Defence Centre of Excellence). Про рівень занепокоєності провідних держав світу у сфері кібербезпеки свідчить і бажання врегулювати на міжнародному рівні можливість визнання кібератаки «актом війни» [53].

Висновки

У результаті здійсненого дослідження можемо резюмувати таке.

Як на міжнародному, так і на національному рівнях відсутнє визначення поняття

«кіберзагрози», і це має негативні наслідки. Проаналізувавши деякі з наявних дефініцій, визначаємо: «кіберзагрози» – протиправні карні дії суб'єктів інформаційних правовідносин, які створюють небезпеку життєво важливим інтересам людини, суспільства й держави загалом, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, а також відносинам щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації. Сутність кіберзагроз становлять їх суб'єкти, тобто суб'єкти інформаційних правовідносин, а об'єктом є безпосередньо інформація. Інформаційні інтервенції становлять суттєву загрозу кібернетичній безпеці. Загрози можуть бути як внутрішні, так і зовнішні. Для розробки дієвого механізму протидії кіберзагрозам Україні варто взяти за приклад наявну практику зарубіжних країн і міжнародної спільноти, привести її у відповідність до українських реалій.

Список використаних джерел:

1. Стратегія національної безпеки України : Указ Президента України від 26.05.2015 № 287/2015 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/287/2015.

2. Дорожня карта Партнерства у сфері стратегічних комунікацій між Радою національної безпеки і оборони України та Міжнародним секретаріатом НАТО [Електронний ресурс]. – Режим доступу : http://mfa.gov.ua/mediafiles/sites/nato/files/Roadmap_Ukr.pdf.

3. Стратегія кібербезпеки України : Указ Президента України від 15.03.2016 № 96/2016 [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/96/2016.

4. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – Вип. 1. – С. 312–320.

5. Лікан В.А. Стратегічні комунікації : [словник] / В.А. Ліпкан, Т.В. Попова ; за заг. ред. В.А. Ліпкана. – К. : О.С. Ліпкан, 2016. – 416 с.

6. Ліпкан В.А. Консолідація інформаційного законодавства України : [монографія] / В.А. Ліпкан, М.І. Дімчогло ; за заг. ред. В.А. Ліпкана. – К. : О.С. Ліпкан, 2014. – 416 с.

7. Ліпкан В.А. Інкорпорація інформаційного законодавства України : [монографія] / В.А. Ліпкан, К.П. Череповський ; за заг. ред. В.А. Ліпкана. – К. : О.С. Ліпкан, 2014. – 408 с.

8. Мандзюк О.А. Стан та перспективи розвитку правового режиму податкової інформації в Україні : [монографія] / О.А. Мандзюк. – К. : Дорадо-Друк, 2015. – 192 с.

9. Баскаков В. Тенденції адміністративної відповідальності у сфері інформаційної безпеки / В. Баскаков, О. Стоєцький // Актуальні проблеми правоохоронної діяльності : матеріали наук.-практ. конф. (Київ, 20 груд. 2010 р.). – К., 2010. – С. 64–66.

10. Дімчогло М.І. Консолідація інформаційного законодавства як напрям боротьби з тероризмом / М.І. Дімчогло // Інформаційні технології боротьби з тероризмом : матеріали наук.-практ. конференції. – К., 2012. – С. 22–24.

11. Залізняк В.А. Інформаційна безпека як інститут інформаційного права України / В.А. Залізняк // Актуальні проблеми зміцнення державності і національної єдності України : матеріали наук.-практ. конференції. – К., 2010. – С. 46–48.

12. Збінський Є.Ф. Захист податкової таємниці як складова інформаційної безпеки / Є.Ф. Збінський // Імперативи розвитку цивілізації. – 2015. – № 2. – С. 84–85.

13. Рудник Л.І. Право на доступ до інформації : дис. ... канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Л.І. Рудник ; Національний університет біоресурсів і природокористування України. – К., 2015. – 247 с.

14. Логінов О.В. Гносеологічний аспект управління інформаційною безпекою України / О.В. Логінов // Науковий вісник Юридичної академії МВС України. – Дніпропетровськ, 2004. – № 2. – С. 153–161.

15. Максименко Ю.Є. Міжнародно-правові та європейські засади забезпечення безпеки інформаційного суспільства / Ю.Є. Максименко // Актуальні проблеми забезпечення національної безпеки України : матеріали наук.-прак. конф. (м. Київ, 6 груд. 2005 р.) / Київський націон. ун-т внутр. справ. – К., 2005. – С. 58–66.

16. Стоєцький О.В. Адміністративна відповідальність за порушення у сфері інформаційної безпеки України : автореф. дис. ... канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / О.В. Стоєцький ; Запорізький нац. ун-т. – Запоріжжя, 2013. – 19 с.

17. Татарникова К.Г. Засади комплексної кодифікації законодавства про інформацію / К.Г. Татарникова // Проблеми державного будівництва в Україні : матеріали XVIII Міжнар. наук.-практ. конф. професорсько-викладацького складу «Україна в Євроінтеграційних процесах» (м. Київ, 16–17 лют. 2013 р.). – К., 2013. – Вип. 21. – Т. 1. – С. 226–229.

18. Череповський К.П. Елементи структуризації міжнародного інформаційного права / К.П. Череповський // Правові та політичні проблеми сучасності : матеріали наук.-практ. конференції. – К., 2012. – С. 40–44.

19. Шепета О.В. Адміністративно-правові засади технічного захисту інформації : автореф. дис. ... канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / О.В. Шепета ; Нац. ун-т Держ. податк. служби України. – Ірпінь, 2011. – 25 с.

20. Арістова І.В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади : дис. ... докт. юрид. наук : 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / І.В. Арістова. – Х., 2002. – 476 с.

21. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти : [монографія] / І.В. Арістова ; за заг. ред. О.М. Бандурки. – Х. : Вид-во Ун-ту внутр. справ, 2000. – 368 с.

22. Цимбалюк В.С. Інформаційне право (основи теорії і практики) : [монографія] / В.С. Цимбалюк. – К. : Освіта України, 2010. – 388 с.

23. Основи інформаційного права України : [навч. посібн.] / [В.С. Цимбалюк, В.Д. Гавловський, В.В. Гриценко та ін.] ; за ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. – К. : Знання, 2004. – 274 с.

24. Цимбалюк В.С. Інформаційне право: концептуальні положення до кодифікації інформаційного законодавства / В.С. Цимбалюк. – К. : Освіта України, 2011. – 426 с.

25. Цимбалюк В.С. Концепція кодифікації законодавства України про інформацію / В.С. Цимбалюк // Інформаційні технології в глобальному управління : матеріали Міжнародної науково-практичної конференції (м. Київ, 29.10.2011). – К. : ФОП Ліпкан О.С., 2011. – С. 73–91.

26. Сопілко І.В. Інформаційні загрози та безпека сучасного українського суспільства / І.В. Сопілко [Електронний ресурс]. – Режим доступу : http://jrnl.nau.edu.ua/index.php/UV/article/viewFile/8181/9770.

27. «Віртуальний ворог»: як захистити бізнес від кібератак? [Електронний ресурс]. – Режим доступу : http://www.polukr.net/uk/blog/2016/08/virtualnyj-voroh-jak-zahistiti-biznes-vid-kiberatak/.

28. Баровська А.В. Функціональний аналіз сфери стратегічних комунікацій / А.В. Баровська, Д.В. Дубов // Стратегічні пріоритети. – 2016. – № 4 (41). – С. 105–112.

29. Проект Стратегії забезпечення кібернетичної безпеки України [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg.pdf.

30. Великий тлумачний словник сучасної української мови / укл. О. Єрошенко. – Донецьк : ТОВ «Глорія Трейд», 2012. – 864 с.

31. Розширення термінології сучасного кіберпростору / [В.В. Куцаєв, Є.О. Живило, С.П. Срібний, Ю.О. Черниш] [Електронний ресурс]. – Режим доступу : mino.esrae.ru/pdf/2014/3Sm/1387.doc.

32. Про Доктрину інформаційної безпеки України : Указ Президента України від 08.07.2009 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/514/2009.

33. Мінін Д.С. Підходи до визначення поняття «кібербезпека» / Д.С. Мінін [Електронний ресурс]. – Режим доступу : http://istfak.org.ua/tendentsii-rozvytku-suchasnoi-systemy-mizhnarodnykh-vidnosyn-ta-svitovoho-politychnoho-protsesu/185-heopolitychna-dumka-ta-heostratehichni-protsesy-v-khkhi-st/971-pidkhody-do-vyznachennya-ponyattya-kiberbezpeka.

34. Рудник Л.І. Право на доступ до інформації : дис. ... канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Л.І. Рудник ; Національний університет біоресурсів і природокористування України. – К., 2015. – 247 с.

35. Діордіца І.В. Інформаційні інтервенції як загроза кібернетичній безпеці / І.В. Діордіца [Електронний ресурс]. – Режим доступу : http://goal-int.org/informacijni-intervencii-yak-zagroza-kibernetichnij-bezpeci/.

36. Єрмоленко В. Голландський референдум про Україну: 5 сценаріїв / В. Єрмоленко [Електронний ресурс]. – Режим доступу : URL: http://www.hromadske.tv/world/gollandskii– referendum-pro-ukrayinu-5-stsenariyiv.

37. Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України» : Указ Президента України від 06.05.2015 [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/287/2015.

38. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт. нарад / упоряд. Д.С. Бірюков, С.І. Кондратов ; за заг. ред. О.М. Суходолі. – К. : НІСД, 2015. – 176 с.

39. Турчинов вимагає швидкої реакції на кіберзагрози, 7 жовтня 2016 р. [Електронний ресурс]. – Режим доступу : http://www.newsru.ua/ukraine/07oct2016/turchinovkiber.html.

40. Климчук О.О. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки / О.О. Климчук, Н.А. Ткачук // Інформаційна безпека людини, суспільства, держави. – 2015. – № 3. – С. 75–83.

41. Мінін Д.С. Підходи до визначення поняття «кібербезпека» / Д.С. Мінін // [Електронний ресурс]. – Режим доступу : http://istfak.org.ua/tendentsii-rozvytku-suchasnoi-systemy-mizhnarodnykh-vidnosyn-ta-svitovoho-politychnoho-protsesu/185-heopolitychna-dumka-ta-heostratehichni-protsesy-v-khkhi-st/971-pidkhody-do-vyznachennya-ponyattya-kiberbezpeka.

42. Кіберзагрози і кібербезпека: чи здатні фахівці протистояти хакерам? 19.09.2016 [Електронний ресурс]. – Режим доступу : http://ukr.obozrevatel.com/news/34918-kiberzagrozi-i-kiberbezpeka-chi-zdatni-fahivtsi-protistoyati-hakeram.htm.

43. SWIFT попередила світові банки про високу кіберзагрозу [Електронний ресурс]. – Режим доступу : http://www.depo.ua/ukr/svit/swift-poperedila-svitovi-banki-pro-visoku-kiberzagrozu-13122016123500.

44. Сенатори США від обох партій виступили із заявою щодо російських кібератак, 12 грудня 2016 р. [Електронний ресурс]. – Режим доступу : http://www.pravda.com.ua/news/2016/12/12/7129541.

45. Countering Information Warfare Act of 2016 [Електронний ресурс]. – Режим доступу : https://www.congress.gov/bill/114th– congress/senatebill/2692/text.

46. Спецслужби США: Росія – кіберзагроза усій життєво важливій інфраструктурі Штатів, 05.01.2017 [Електронний ресурс]. – Режим доступу : http://zik.ua/news/2017/01/05/spetssluzhby_ssha_rosiya__kiberzagroza_usiy_zhyttievo_vazhlyviy_infrastrukturi_1021403.

47. Розвідка США назвала Росію головною кіберзагрозою, 05.01.2017 [Електронний ресурс]. – Режим доступу : http://www.pravda.com.ua/news/2017/01/5/7131747.

48. Російська кіберзагроза, 26 вересня 2016 р. [Електронний ресурс]. – Режим доступу : http://www.radiosvoboda.org/a/28014684.html.

49. Європейський парламент ухвалив резолюцію щодо протидії російській пропаганді, 23.11.2016 [Електронний ресурс]. – Режим доступу : http://glavcom.ua/news/jevropeyskiy-parlament-uhvaliv-rezolyuciyu-shchodo-protidiji-rosiyskiy-propagandi-384228.html.

50. Порошенко закликав США «бути великими знову», 19.01.2017 [Електронний ресурс]. – Режим доступу : http://www.pravda.com.ua/news/2017/01/19/7132837.

51. У Міноборони анонсували створення Центру реагування на кіберзагрози, 30.11.2016 [Електронний ресурс]. – Режим доступу : http://www.unian.ua/society/1653082-u-minoboroni-anonsuvali-stvorennya-tsentru-reaguvannya-na-kiberzagrozi.html.

52. НБУ і НАБУ створять центр реагування на кіберзагрози в банківській системі, 04.10.2016 [Електронний ресурс]. – Режим доступу : http://wz.lviv.ua/news/184233-nbu-i-nabu-stvoriat-tsentr-reahuvannia-na-kiberzahrozy-v-bankivskii-systemi.

53. Сучасні тренди кібербезпекової політики: висновки для України [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/articles/294.

В статье исследовано понятие и содержание киберугроз на современном этапе. Акцентировано внимание на том, что как на международном, так и на национальном уровнях отсутствует определение понятия «киберугрозы», и это имеет негативные последствия. Предложено авторское понимание термина: «киберугрозы» – противоправные уголовные действия субъектов информационных правоотношений, которые создают опасность жизненно важным интересам человека, общества и государства в целом, реализация которых зависит от надлежащего функционирования информационных, телекоммуникационных и информационно-телекоммуникационных систем, а также отношениям по созданию, сбору, получению, хранению, использованию, распространению, охраны, защиты информации. Указано, что сущность киберугроз составляют их субъекты, то есть субъекты информационных правоотношений, а объектом является непосредственно информация. Информационные интервенции составляют существенную угрозу кибернетической безопасности. Отмечено, что угрозы могут быть как внутренние, так и внешние. Для разработки действенного механизма противодействия киберугрозам Украине предложено взять за пример существующую практику зарубежных стран и международного сообщества и привести ее в соответствие к украинским реалиям.

Ключевые слова: кибербезопасность, информационная интервенция, киберугрозы, хактивисты, кибераграсия, информация, киберпространство.

It was noted that, there is no definition of "cyber threats" both at international and national levels and it has negative consequences. After analyzing some of the existing definitions, the author's understanding of "cyber threats" was offered – it is illegal criminal actions of the subjects of information relations that create the danger to the vital interests of man, society and the state as a whole, the implementation of which depends on the proper functioning of information and telecommunication systems as well as information and telecommunication systems, and relations concerning the creation, collection, receipt, possession, use, distribution, security and protection of information. It was marked that subjects, ie subjects of legal information relations, and the object (the information) disclose the content of the cyber threats. It was argument that information interventions constitute a significant threat to the cyber security. Threats can be both internal and external. It was stated that Ukraine should take as an example the current practice of foreign countries and the international community and bring it into line with the Ukrainian realities to develop an effective mechanism for combating of the cyber threads.

Key words: cyber security, informational intervention, cyber threats, hactivists, cyber aggression, information, cyber space.