УДК 343.32

Ігор Діордіца,
канд. юрид. наук, доцент,
доцент кафедри кримінального права і процесу
Національного авіаційного університету

КЛАСИФІКАЦІЯ КІБЕРЗАГРОЗ ТА ЇХ ЛЕГІТИМАЦІЯ У НОРМАТИВНО-ПРАВОВИХ АКТАХ УКРАЇНИ

У статті автором досліджено класифікації кіберзагроз та їх легітимацію у НПА. Зауважено, що захист критичної інфраструктури від кібернетичних загроз повинен бути складником загальнодержавної системи кібернетичної безпеки, а для протидії сучасним загрозам у кіберпросторі система захисту повинна мати змогу швидко адаптуватися до змін. Акцентовано увагу на тому, що в наявних нормативно-правових актах відсутня дефініція «кіберзагроза». Запропоновано авторське розуміння терміна «легітимація кіберзагроз» та «загрози кібербезпеці або кіберзагрози». Зазначено, що за відсутності єдиного уніфікованого визначення кіберзагроз, актуальним є перегляд чинних нормативно-правових актів та їх доповнення. Нині існує низка НПА, в яких вживається термін «кіберзагроза», але не дається його тлумачення, що може призвести до його неправильного застосування, помилок у притягненні до відповідальності та інших негативних наслідків. Основними видами кіберзагроз є: кіберзлочинність; кібертероризм та кібершпигунство; кібервійна.

Ключові слова: кіберзлочинність, кібертероризм, кібершпигунство, кіберпростір, кіберзагроза, легітимація, кібервійна.

Важливість кіберпростору для життя сучасного суспільства є очевидною, зважаючи не лише на такі показники, як кількість користувачів мережі Інтернет та динаміка їх збільшення, але й на поступове проникнення його у решту сфер людського життя. Нині використання мережевих можливостей та технологій стає все більш очевидним для політики і безпеки держави. Якщо у світі сьогодні ще зберігається стратегічний баланс у сфері звичайних озброєнь та зброї масового знищення, то питання паритету в кіберпросторі залишається відкритим, а якщо бути відвертим, то паритету вже не існує.

Підтвердженням цього є активність спеціальних підрозділів окремих держав, громадських і терористських організацій, яка націлена на використання кіберпростору для досягнення різноманітних соціально-політичних, економічних, інформаційних та військових цілей. Промовистими свідченнями важливості мережевих технологій є також так звані «кольорові» революції, події «арабської весни» та численні інспіровані ззовні кризи, що відбувалися у багатьох країнах світу [1, с. 241].

Мета статті. Коли йдеться про кібербезпеку, традиційно намагаються підкреслити нові, специфічні загрози, що характерні для сучасного стану розвитку інформаційно-комунікаційних технологій і рівня впровадження їх у повсякденне життя. Тому актуальним завданням є визначення поняття «кіберзагроза», відповідна класифікація та легітимація у нормативно-правових актах. Відтак мета даної статті – дослідити класифікацію кіберзагроз та їх легітимацію у нормативно-правових актах (далі —НПА).

Питання кібернетичної безпеки вже поступово стає предметом дослідження українських учених. Проте звертають на нього увагу насамперед фахівці з питань національної безпеки та представники юридичної науки, зокрема Четверик Г. Г. [1], Попова Т. В., Ліпкан В. А. [2-5], Рудник Л. І. [6-7], Діордіца І. В. [8-13], Лахно В. А. [14], Панченко В. М. [15] та ін. При цьому це відбувається або на рівні окремих наукових статей або на рівні монографічних досліджень, де кібернетична безпека не виступає основним предметом розгляду. Окрім цього, зазначу, що натепер в Україні з юридичних наук не захищено жодної дисертації з порушених питань, незважаючи на нагальність наукового вивчення даної проблеми.

Виклад основного матеріалу. Ефективність функціонування сучасних систем та технологій виявлення кібератак (кіберзагроз – авт.) істотно залежить від оперативності та достовірності моніторингової інформації про активність кіберзлочинців на попередніх стадіях реалізації атак на інформаційні ресурси, зокрема й критично важливі. Як показав проведений мною аналіз світового досвіду, натепер найбільш ефективним методологічним підходом до побудови інноваційних інтелектуальних моніторингових систем кібернападів є створення ієрархічних багаторівневих структур розпізнавання кібератак (кіберзагроз – авт.) на початкових стадіях їх реалізації. При цьому ієрархічний підхід дає змогу розв'язувати складні задачі управління процесом захисту інформації від кібератак у розподілених критично важливих інформаційних системах як послідовність локальних задач, скоординованих між собою [14, с. 18].

Стрімке впровадження інформаційних технологій у всі сфери життєдіяльності сус-

пільства, глобалізація інформаційних відносин викликали занепокоєність станом кібернетичної безпеки об'єктів критичної інфраструктури й у світового співтовариства. Про актуальність цієї проблеми для України свідчить рішення Ради національної безпеки і оборони України від 17 листопада 2010 р. «Про виклики та загрози національній безпеці України у 2011 році». Одним із пріоритетних завдань, визначених у цьому документі, є побудова єдиної загальнодержавної системи протидії кіберзлочинності, що має забезпечити захист критичної інфраструктури. Адже нині законодавством України встановлено лише окремі об'єкти соціально-економічної сфери, надзвичайні події на яких можуть призвести до суспільно небезпечних наслідків, тоді як єдиний порядок ідентифікації та класифікації об'єктів критичної інфраструктури не розроблено. Нормативно не визначеною залишається низка основоположних термінів у сфері захисту критичної інфраструктури від кіберзагроз, зокрема і поняття «критична інфраструктура». Потребує наукового обґрунтування механізм організації діяльності та взаємодії державних органів і приватних структур у процесі захисту критичної інфраструктури [15, с. 91].

Основними етапами формування системи захисту національної інфраструктури від кіберзагроз є:

1) визначення основних понять та їх нормативне закріплення;

2) визначення критеріїв віднесення об'єктів до критично важливих;

3) укладання переліку таких об'єктів;

4) оцінка ризиків безпеки (здійснювалася або централізовано, або галузевими міністерствами відповідно до єдиної методики, розробленої науковими установами на замовлення державних органів);

5) планування заходів безпеки на основі результатів оцінювання ризиків із метою оптимізації витрат [15, с. 96].

Саме тому і зупинимося на визначенні основних понять та їх нормативному закріпленні, а саме поняття «кіберзагроза».

Перш за все визначимося із категорією «легітимація». У тлумачному словнику української мови дається така дефініція терміна «легітимація» – визнання чи підтвердження законності якого-небудь права або повноваження; узаконення позашлюбних дітей; спосіб або процес, завдяки якому держава або політична система одержує виправдання; форма посвідчення особи громадянина в державах, де відсутня паспортна система [16, с. 322]. Ці тлумачення не зовсім кореспондують з об'єктом нашого дослідження, тому звернемося до спеціалізованих джерел. Так, В. А. Ліпкан та О. С. Ліпкан пропонують визначати легітимацію як процес узаконення [3, с. 183], тобто під *«легітимацією кіберзагроз»* варто розуміти їх узаконення або закріплення у нормативно-правових актах, що сприятиме, по-перше, визначенню переліку кіберзагроз, по-друге, розкриттю їх сутності, потретє, виробленню варіантів їх відвернення та ліквідації їх негативних наслідків.

Зауважу, що в чинних нормативно-правових актах відсутня дефініція «кіберзагроза». Із наявних напрацювань зазначу таке: *кібернетична загроза (кіберзагроза)* – наявні та потенційно можливі явища і чинники, що створюють небезпеку інтересам людини, суспільства та держави через порушення доступності, повноти, цілісності, достовірності, автентичності режиму доступу до інформації, яка циркулює в критичних об'єктах національної інформаційної інфраструктури [17].

Беручи до уваги той факт, що кібербезпека наразі розглядається як складова частина інформаційної безпеки, зауважу, що «загрози інформаційній безпеці» – наявні та потенційно можливі явища і чинники, які створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави в інформаційній сфері [18], відповідно, *«загрози кібербезпеці, або кіберзагрози»* – наявні та потенційно можливі явища і чинники, які створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави в кібернетичній сфері.

Ще одна доктринальна дефініція запропонована В. А Ліпканом у першому словнику зі Стратегічних комунікацій : *«кіберзагроза»* – дестабілізуючий чинник негативного впливу на об'єкт інформаційної безпеки шляхом використання технологічних можливостей кіберпростору, спрямованих на порушення конфіденційності, цілісності, авторства, спостережності та доступності інформації; загроза застосування деструктивних інформаційно-психологічних впливів на свідомість та психічний стан населення [2, с. 190].

У цьому визначенні виникла ще одна невідома категорія, а саме *«спостережність»* – властивість комп'ютерної системи, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів для запобігання порушенню політики безпеки та/або забезпечення відповідальності за певні дії [2, С. 346].

Також під *«спостережністю»* пропонується розуміти властивість ІКС, що дає змогу фіксувати діяльність користувачів і яка використовується з метою запобігання порушенню політики безпеки і (або) забезпеченню відповідальності за певні дії [19].

«Кіберзагроза» – протиправні, карані дії суб'єктів інформаційних правовідносин, які створюють небезпеку життєво важливим інтересам людини, суспільства та держави в цілому, 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 [11].

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

Таким чином, за відсутності єдиного уніфікованого визначення кіберзагроз актуальним є перегляд чинних нормативно-правових актів та їх доповнення. Нині існує низка НПА, в яких вживається термін «кіберзагроза», але не дається його тлумачення, що може призвести до його неправильного застосування, помилкового притягнення до відповідальності та інших негативних наслідків.

Усі види кіберзагроз виникали і поширювалися з розвитком Інтернету та його проникненням у суспільне, політичне та економічне життя нашого суспільства.

Факторами, які зумовили створення систем захисту критичної інфраструктури від кібернетичних загроз, є:

– кількісне та якісне зростання кіберзагроз;

– поява нових вразливостей у процесі технологічного розвитку інформаційно- телекомунікаційних систем;

– неспроможність ринкових механізмів гарантувати захист від кіберзагроз;

– збільшення взаємозалежності елементів інфраструктури, внаслідок чого порушення нормального функціонування одних секторів критичної інфраструктури викликає проблеми в інших [15, с. 96].

Джерелами кібернетичних загроз можуть бути міжнародні злочинні групи хакерів, окремі підготовлені у сфері інформаційних технологій злочинці, іноземні державні органи, терористичні та екстремістські угруповання, транснаціональні корпорації та фінансово-промислові групи тощо [17].

Як зазначено у Проекті Стратегії забезпечення кібернетичної безпеки України [17], *основними видами кіберзагроз* (загроз у сфері кібернетичної безпеки) є: кіберзлочинність; кібертероризм та кібершпигунство; кібервійна.

Окремо зупинюсь на кожній із даних категорій. *«Кіберзлочинність»* – протиправне втручання в роботу кібернетичних систем, основною управляючою ланкою яких є комп'ютер (наприклад, спотворення інформації про стан об'єкта в каналі зворотного зв'язку, спотворення керуючого сигналу й каналу зв'язку, використання шкідливого програмного забезпечення тощо), створення та використання в злочинних цілях певної кібернетичної (комп'ютерної) системи, використання в злочинних цілях існуючих кібернетичних (комп'ютерних) систем (наприклад, шахрайство у комп'ютерних чи телекомунікаційних мережах, вимагання тощо) [20, с. 85].

Злочини з використанням сучасних інформаційно-телекомунікаційних технологій стають дедалі звичнішою практикою в житті українських громадян. Причому новітні технології застосовуються не лише для скоєння традиційних видів злочинів, але й для скоєння нових видів злочинів, характерних, передусім, для розвинутого інформаційного суспільства. Найбільша увага злочинців зосереджена на спробах порушення роботи або несанкціонованого використання можливостей інформаційних систем державного, кредитно-банківського, комунального, оборонного, виробничого секторів. Усе ще актуальними залишаються проблеми боротьби з дитячою порнографією та порушеннями авторських та суміжних прав [17].

Визначення *інформаційного або кібертероризму* можна знайти як у міжнародно-правових документах та проектах конвенцій, так і в дослідженнях фахівців із цієї проблематики. Однією з характерних рис визначень інформаційного тероризму є те, що здебільшого в них згадується тільки один аспект інформаційної безпеки, а саме пов'язаний із засобами оброблення інформації, що звужує поняття інформаційного тероризму, тим самим обмежуючи сферу правового регулювання, що не сприяє ефективній співпраці держав у справі боротьби з інформаційним тероризмом. *«Кібертероризм»* – протиправне діяння, яке вчиняється з метою досягнення негативних наслідків, наприклад отримання матеріальних благ чи загрози інформаційній безпеці держави. Кібертероризм має місце в кібербезпековому просторі [12].

Кібершпигунство, або комп'ютерний шпіонаж (вживається також термін «*кіберрозвідка*») – термін, що позначає, як правило, несанкціоноване отримання інформації з метою отримання особистої, економічної, політичної чи військової переваги, здійснюване з використанням обходу (злому) систем комп'ютерної безпеки, із застосуванням шкідливого програмного забезпечення, включаючи «троянських коней» і шпигунських програм. Під «*кібершпигунством*» пропонується розуміти – злочинну діяльність, яка здійснюється шляхом таємного вистежування, розшуку, збирання, викрадання та передачі інформації, що становить державну таємницю, іноземній державі, іноземній організації або їх представникам, якщо ці дії вчинені іноземцем або особою без громадянства і з використанням кібернетичного простору [13].

Ціла низка вітчизняних підприємств, порушення роботи яких може становити загрозу життю та здоров'ю громадян, може стати потенційною ціллю для здійснення терористичних актів у тому числі із застосуванням сучасних інформаційних технологій. Не меншою загрозою є вчинення протиправних дій на шкоду третім країнам, що здійснюються із використанням вітчизняної інформаційної інфраструктури і загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем. Інформація з обмеженим доступом, що циркулює в національних інформаційних ресурсах, є постійним об'єктом зацікавленості з боку інших держав, організацій та осіб. Крім того, все більшого поширення набуває політично вмотивована діяльність у кіберпросторі груп активістів (хактивістів), які здійснюють атаки на урядові та приватні сайти, що призводить до порушень роботи інформаційних ресурсів, а також репутаційних та матеріальних збитків [17].

Останнім часом кіберпростір перетворюється на арену боротьби між суб'єктами міжнародних відносин. За цих умов набув поширення термін «кібервійна». Однак цей термін не є усталеним.

Дослідниками та експертами пропонується широкий спектр визначень ***кібервійни,*** зокрема:

кібервійна – чітко скоординована цифрова атака однієї держави, спрямована на проникнення у комп'ютери та мережі іншої держави, з метою завдання шкоди або руйнування;

кібервійна – конфлікт, що передбачає використання ворожих, незаконних атак на комп'ютери та мережі з метою руйнування комунікацій та інших елементів інфраструктури як механізм завдання економічної шкоди або підриву системи оборони країни;

кібервійна – застосування комп'ютерних технологій та мережі Інтернет однією державою (або за її безпосередньої підтримки) проти іншої держави, спрямоване проти її безпеки й оборони, яке є настільки інтенсивним і серйозним, що становить реальну загрозу безпеці та суверенітету цієї іншої держави [21, с. 81].

Воєнна сфера зазнає чи не найдраматичніших змін внаслідок розбудови глобального кіберпростору. Більшість країн світу активно трансформує свої потенціали у сфері оборони в напрямі посилення кібернетичних можливостей ведення бойових дій та захисту від аналогічних дій з боку супротивника, оскільки все актуальнішими стають нові типи загроз. З урахуванням широкої інформатизації сектору безпеки і оборони, зокрема створення ЄАСУ ЗС України, оборонний потенціал нашої держави стає більш чутливим до кіберзагроз. Упровадження провідними країнами сучасних кіберозброєнь перетворює кіберпростір на окрему, поряд із традиційними «Земля», «Повітря», «Море», «Космос», сферу ведення бойових дій, а у найближчому майбутньому рівень обороноздатності країни буде визначатись у т. ч. наявністю у неї ефективних підрозділів для ведення бойових дій у кіберпросторі та здатністю протистояти кіберзагрозам у сфері оборони [17].

Загрози кібербезпеці актуалізуються через дію таких чинників, зокрема, як:

– невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;

– недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;

– безсистемність заходів кіберзахисту критичної інформаційної інфраструктури;

– недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів;

– недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;

– недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки [22].

Джерелами загроз та викликів національній безпеці України в інформаційній сфері можуть бути міжнародні злочинні групи хакерів, окремі підготовлені у сфері ІТ злочинці, іноземні державні органи, терористичні угруповання, недержавні організації, політичні структури та неформальні об'єднання екстремістського спрямування, транснаціональні корпорації та фінансово-промислові групи тощо. Зростає загроза використання проти інтересів України кібернетичних засобів як із середини держави, так і з-за меж її кордонів. Такою ж реальною є загроза використання української інформаційної інфраструктури як «транзитного майданчику» для приховування атаки на інформаційні ресурси третьої сторони, що може розцінюватись провідними країнами як дії держави з відповідними наслідками політичного, економічного, правового, а в перспективі, не виключено, і воєнного характеру [23].

Мережеві загрози також діляться на три види.

Програмно-технічні загрози стали першим видом загроз, що викликала панічні настрої як приватних користувачів, так і представників великих бізнес структур, а також державних органів.

Економічні загрози – наступна проблема. Після того як у мережу прийшов бізнес, стали популярні системи інтернет-платежів, пожвавилася електронна торгівля, з'явилися системи інтернет банкінгу.

Актуальними стали зломи платіжних аккаунтів, фішинг-атаки, продаж номерів кредитних карт. Усі учасники ринку зайнялися розробкою систем захисту від економічних кіберзагроз, а також правил поводження з грошима в інтернеті.

Після того як публікація контенту, як текстового, так і фото-, відео-, стала доступна кожному, з'явилися так звані *контентні кіберзагрози* і, відповідно, новий підвид кібербезпеки – контентної безпеки.

До контентних загроз належить поширення матеріалів, що порушують законодавство. До останніх належать:

– дитяча порнографія;

– сексуальна експлуатація неповнолітніх і діяльність педофілів;

– терористична і екстремістська інформація;

– сектантська інформація;

– злочини проти персональних даних, честі та гідності особи;

наркопропаганда;

насильство в інтернеті, пропаганда злочинів та навчання щодо їх скоєння.

Аналітики вважають, що акцент на вплив порнографії відвертає суспільну увагу від інших кіберзагроз, наслідки яких можуть бути набагато серйознішими. Сьогодні більшу актуальність становлять загрози, пов'язані з поширенням матеріалів екстремістського змісту, ксенофобських матеріалів, а також пропаганда злочинів, пов'язаних із наркотиками і тероризмом [24].

Кіберзагрози також можна поділити на такі ***види:***

таргетовані атаки (advanced persistent threat). Залежно від цілей можна виділити дві протилежні тактики атак на комп'ютерні системи. Перший варіант – застосувати для атаки програмне забезпечення (вірус, троян-

ський кінь), маючи на меті компрометацію якомога більшої кількості систем. Другий варіант – проводити атаку прицільно (звідки й назва «таргетовані», тобто націлені) для компрометації комп'ютерів конкретної установи або навіть конкретних користувачів (як правило, посадових осіб високого рангу або їхніх помічників, науковців, взагалі людей, які мають справу з особливо цінною інформацією);

– *кібертероризм* (вплив на системи керування). Те, що називають власне кібертероризмом, – можливість впливу через комп'ютерну мережу (зокрема, Інтернет) на системи керування транспортом, промисловими об'єктами, будинками та будь-якими технологічними процесами. ІКТ надають терористам кілька інструментів: застосування комп'ютерних мереж для керування, координації дій і підготовки терактів; можливість терористів напряму звертатись до широкого кола людей, використовуючи сервіси сучасного Інтернету; потенційно будь-який технологічний процес, яким керує цифрова система керування (або SCADA), може стати об'єктом атаки кібертерористів;

– *кібервійни*. Stuxnet – це є прообраз кіберзброї для ведення кібервійни, використовується для здійснення диверсій або відключення систем (наприклад, комплексів протиповітряної чи протиракетної оборони);

– *хактивізм* – зловживання інформацією у соціальних мережах (вплив на суспільство). Деякі хакерські угруповання ставлять за мету видобування конфіденційної (іноді таємної) інформації і розкриття її шляхом розміщення в Інтернеті у вільному доступі. Як правило, йдеться про викриття таємних операцій, змов, корупції та інших дій на рівні урядів чи окремих політичних сил, які суперечать закону, принципам демократії й іншим загальнолюдським цінностям;

– *атаки на банківські системи* (викрадення грошей). Чим ширше у банківській сфері застосовуються інформаційно-комунікаційні технології, тим більше можливостей для махінацій у цій сфері. Дуже поширеними є фішинг, викрадення і використання атрибутів платіжних карток, а також застосування дуже складного і досконалого шкідливого програмного забезпечення для втручання в роботу систем клієнт-банк;

– *атаки на електронний уряд*. «Електронний уряд» – інформаційно- комунікаційна система, або об'єднання інформаційно-комунікаційних систем, що автоматизує інформаційну взаємодію органів державної влади та органів місцевого самоврядування з громадянами та суб'єктами господарювання з метою підвищення ефективності надання державних послуг. Атаки на електронний уряд можуть зашкодити функціонуванню такої системи, а у країнах з низьким рівнем впровадження інформаційно-комунікаційних технологій – підірвати довіру до демократичних перетворень і технічного прогресу;

– *апаратні закладки* у мікросхемах і прошивках комп'ютерного і мережного обладнання [25, с. 17].

Таким чином, резюмуючи вищезазначене, можна *висновувати,* що проблема захисту критичної інфраструктури від кібернетичних загроз повинна бути складовою частиною загальнодержавної системи кібернетичної безпеки. Для протидії сучасним загрозам у кіберпросторі системи захисту повинні мати змогу швидко адаптуватися до змін. У чинних нормативно-правових актах відсутня дефініція «кіберзагроза». Під «легітимацією кіберзагроз» варто розуміти їх узаконення або закріплення у нормативно правових актах. «Загрози кібербезпеці або кіберзагрози» – наявні та потенційно можливі явища і чинники, які створюють небезпеку для життєво важливих інтересів людини і громадянина, суспільства і держави в кібернетичній сфері. За відсутності єдиного уніфікованого визначення кіберзагроз актуальним є перегляд чинних нормативно-правових актів та їх доповнення. Нині існує низка НПА, в яких вживається термін «кіберзагроза», але не дається його тлумачення, що може призвести до його неправильного застосування, помилок у притягненні до відповідальності та інших негативних наслідків. Основними видами кіберзагроз (загроз у сфері кібернетичної безпеки) є: кіберзлочинність; кібертероризм та кібершпигунство; кібервійна.

Список використаних джерел:

1. Четверик Г. Г. Напрямки реалізації державної політики у сфері кібернетичної безпеки / Г. Г. Четверик // Вісник Дніпропетровського університету. – 2012. – Вип 22. – С. 240–245.

2. Стратегічні комунікації : словник / [Т. В. Попова, В. А. Ліпкан] ; за заг. ред. доктора юридичних наук В. А. Ліпкана. – К. : ФОП Ліпкан О.С., 2016. – 416 с.

3. Ліпкан В. А. Національна і міжнародна безпека у визначеннях та поняттях / В. А. Ліпкан, О. С. Ліпкан. – 2-ге вид., доп. і перероб. – К.: Текст, 2008. – 400 с.

4. Ліпкан В. А. Національна безпека України : навчальний посібник / В. А. Ліпкан. – 2-ге вид. – К. : КНТ, 2009. – 576 с.

5. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. – К. : КНТ, 2006. – 280 с.

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

7. Рудник Л. І. Роль та місце стратегічних комунікацій в сучасному суспільстві знань / Л. І. Рудник [Електронний ресурс]. – Режим доступу : http://goal-int.org/rol-ta-mistse-strategichnih-komunikatsij-v-suchasnomu-suspilstvi-znan/

8. Діордіца І. В. Поняття та зміст кіберзлочинності / І. В. Діордіца [Електронний ресурс]. – Режим доступу : http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti/

9. Діордіца І. В. Сучасний кібертероризм: аспекти правового регулювання /

І. В. Діордіца [Електронний ресурс]. – Режим доступу : http://goal-int.org/suchasnij-kiberterorizm-aspekti-pravovogo-regulyuvannya/

10. Діордіца І. В. Система забезпечення кібербезпеки: сутність та призначення / І. В. Діордіца // [Електронний ресурс]. – Режим доступу : http://goal-int.org/sistema-zabezpechennya-kiberbezpeki-sutnist-ta-priznachennya/

11. Діордіца І. В. Поняття та зміст кіберзагроз на сучасному етапі / І. В. Діордіца [Електронний ресурс]. – Режим доступу : http://goal-int.org/ponyattya-ta-zmist-kiberzagroz-na-suchasnomu-etapi/

12. Діордіца І. В. Кібертероризм як елемент дестабілізації системи стратегічних комунікацій / І. В. Діордіца [Електронний ресурс]. – Режим доступу : http://goal-int.org/kiberterorizm-yak-elementi-destabilizacii-sistemi-strategichnix-komunikacij/

13. Діордіца І. В. Поняття та зміст кібершпигунства / І. В. Діордіца [Електронний ресурс]. – Режим доступу : http://goal-int.org/ponyattya-ta-zmist-kibershpigunstva/

14. Лахно В. А. Побудова адаптивної системи розпізнавання кіберзагроз на основі нечіткої кластерізації ознак / В. А. Лахно // Восточно-Европейский журнал передовых технологий. – 2016. – № 2(9). – С. 18–25.

15. Панченко В. М. Зарубіжний досвід формування систем захисту критичної інфраструктури від кіберзагроз / В. М. Панченко // Інформаційна безпека людини, суспільства, держави : наук.-практ. журн. – К. 2012. – №3 (10). – С. 100–109.

16. Великий тлумачний словник сучасної української мови /г. ред. В.Т. Бусел, редактори-лексикографи: В.Т. Бусел, М.Д. Василега-Дерибас, О.В. Дмитрієв та ін. – К.: Ірпінь: ВТФ «Перун», 2005. – 1728 с.

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

18. Проект Концепції інформаційної безпеки України [Електронний ресурс]. – Режим доступу : http://www.osce.org/uk/fom/175056?download=true

19. «Спостережність» // Електронний словник [Електронний ресурс]. – Режим доступу : http://wiki.tntu.edu.ua

20. Словник термінів з кібербезпеки / за заг. ред. О. Копана, Є. Скулиша. – К. : ВБ «Аванпост-Прим», 2012. – 214 с.

21. Запорожець О. Ю. Кібервійна: концептуальний вимір / О. Ю. Запорожець // Актуальні проблеми міжнародних відносин / ред. В. В. Копійка. – Вип. 121. – Частина І. – К. : Ін-т МВ КНУ ім. Т. Г. Шевченка, 2014. – 232 с.

22. Стратегія кібербезпеки України від 15.03.2016 [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/96/2016

23. Косогов О. М. Пріоритетні напрямки державної політики щодо забезпечення безпеки національного кіберпростору / О. М. Косогов // Збірник наукових праць Харківського університету Повітряних Сил. – 2014. – Вип. 3. – С. 127–130.

24. Екстремізм і ксенофобія небезпечніше порнографії [Електронний ресурс]. – Режим доступу : https://www.dobrenok.com/ua/news/4430-ekstremizm-i-ksenofobiya-pornografiyi.html

25. Грайворонський М. В. Сучасні підходи до забезпечення кібернетичної безпеки / М. В. Грайворонський // Матеріали XIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», м. Київ, 21-23 травня 2015. – Київ : НТУУ «КПІ», 2015. – С. 10–17.

В статье автором исследованы классификации киберугроз и их легитимация в НПА. Отмечено, что защита критической инфраструктуры от кибернетических угроз должна быть составляющей общегосударственной системы кибернетической безопасности, а для противодействия современным угрозам в киберпространстве система защиты должна иметь возможность быстро адаптироваться к изменениям. Акцентировано внимание на том, что в существующих нормативно-правовых актах отсутствует дефиниция «киберугроза». Предложено авторское понимание терминов «легитимация киберугроз» и «угрозы кибербезопасности, или киберугрозы». Отмечено, что при отсутствии единого унифицированного определения киберугроз актуальным является пересмотр существующих нормативно-правовых актов и их дополнение. В настоящее время существует ряд НПА, в которых употребляется термин «киберугроза», но не дается его толкование, что может привести к его неправильному применению, ошибкам в привлечении к ответственности и другим негативным последствиям. Основными видами киберугроз являются: киберпреступность; кибертерроризм и кибершпионаж; кибервойна.

Ключевые слова: киберпреступность, кибертерроризм, кибершпионаж, киберпространство, киберугрозы, легитимация, кибервойна.

It was marked that the problem of the protecting of the critical infrastructure from the cyber threats must be a part of the nationwide system of the cyber security. The security system must be able to adapt quickly to changes in order to counter current threats in the cyberspace. The attention was paid to the fact there is no definition of "cyber threats" in the existing regulatory acts. It was offered to understand under "Legitimation of the cyber threats" their legalization or consolidation in the regulatory acts, what will, firstly, help to determine the list of cyber threats, secondly, to reveal their essence, thirdly, to develop options for their diversion and elimination of their negative consequences. "Threats to cybersecurity or cyber threats" were determined as available and potentially possible phenomena and factors that create danger to the vital interests of man and citizen, society and the state in the cyber sphere. It was marked that the content or the essence of cyber threats is disclosed by their subjects, namely, the subjects of information legal relations, and the object is information. Thus, in the absence of the single unified definition of the cyber threats, the review of existing regulations and their additions is relevant. Currently, there are a number of regulations that use the term "cyber threats" but do not give their interpretation, that can lead to its misuse, prosecution and other negative consequences. It was stated that the main types of cyber threats (threats in the field of cyber security) are: cybercrime; cyberterrorism and cyber-espionage; cyberwarfare.

Key words: cybercrimes, cyberterrorism, cyber-espionage, cyberspace, cyberthreats, legitimation, cyberwarfare.