РОЛЛЕР В. М.,
ад'юнкт
(Військовий інститут
Київського національного університету
імені Тараса Шевченка)

УДК 342.9. 34.07

ПРАВОВЕ РЕГУЛЮВАННЯ ЗДІЙСНЕННЯ КІБЕРОБОРОНИ

Питання функціонування та правового регулювання діяльності у віртуальному середовищі привертають до себе все більше уваги у світовій спільноті. Загрози, що несе кіберпростір, такі як кібератаки, викликають необхідність проведення заходів з кіберзахисту, а в деяких випадках і кібероборони уповноваженими органами держав. Стаття присвячена вивченню питання правового регулювання здійснення заходів кібероборони в Україні.

Ключові слова: *правове регулювання, кіберпростір, кіберзахист, кібероборона.*

Вопросы функционирования и правового регулирования деятельности в виртуальной среде привлекают к себе все больше внимания в мировом сообществе. Угрозы, которые несет киберпространство, такие как кибератаки, вызывают необходимость проведения мероприятий по защите от киберугроз, а в некоторых случаях и кибероборонны уполномоченными органами государств. Статья посвящена изучению вопросов правового регулирования осуществления мероприятий кибероборонны в Украине.

Ключевые слова: *правовое регулирование, киберпространство, киберзащита, кибероборона.*

The question of the functioning and legal regulation of activities in the virtual environment attract more and more attention in the world community. Threats that carry the cyberspace, such as cyberattacks, call for cyber defense measures to be taken, and in some cases also cyber-security actions by the authorities. The article is devoted to the study of the legal regulation of the implementation of measures of the cyber defense in Ukraine.

Key words: *legal regulation, cyberspace, cyber defense, cyber defense.*

Вступ. До питань забезпечення кібербезпеки держави звертаються все більше спеціалістів, юристів, науковців і політиків. Але це й не дивно, оскільки це нова сфера суспільних відносин, де учасники: держава та суспільство – нерозривно пов'язані.

Сама сфера цих відносин і їх правове регулювання лише починають формуватися, хоча фактичні суспільні відносини в цій сфері розвиваються дуже динамічно. Законодавча база не є достатньо розвиненою, а ті нормативно-правові акти, що існують натепер, не дають відповіді для адекватного регулювання відносин. Не є юридично визначеними суб'єкти, які здійснюють діяльність у кіберпросторі.

У цьому аспекті ведення бойових дій у кібернетичному просторі (кібервійни, кібернетичні операції) можна вважати одним із основних напрямів революції у військовій площині, який, тим не менше, ставить багато питань перед науковцями в галузі права.

Питання правового регулювання кібербезпеки та протидії кіберзлочинності вивчають О.А. Баранов, Ю.Н. Батурин, П.Д. Біленчук.

Постановка завдання. Мета статті – вивчити питання правового регулювання здійснення заходів кібероборони в Україні.

Результати дослідження. Щодо визначення кіберпростору. У 2003 році на 32-й сесії Генеральної конференції ЮНЕСКО прийнято рекомендацію «Про розвиток та використання багатомовності та загальному доступі до кіберпростору», згідно з якою кіберпростір визначається як віртуальний світ цифрової та електронної комунікації, пов'язаної з глобальною інформаційною інфраструктурою [1].

У світовій правозастосовній практиці поняття «кіберпростір» почало зустрічатися з кінця XX ст. У цьому контексті показовим є визначення кіберпростору, що здійснене Верховним судом США, – це унікальний носій, відомий його користувачам як кіберпростір, що не знаходиться на певній території, але доступний кожному в будь-якій точці світу через Інтернет [2].

Зрештою, у 2013 році Північноатлантичним альянсом опубліковано Талліннське керівництво з міжнародного права щодо методів ведення кібернетичних бойових дій, яким кіберпростір визначено як середовище, що сформовано з фізичних і нефізичних елементів і характеризується використанням комп'ютерів та електромагнітного спектру для зберігання, зміни й обміну даними з використанням комп'ютерних мереж [3].

Отже, кіберпростір можна охарактеризувати як специфічне середовище, яке хоча і створено людиною, але через свою глобалізацію отримало такий значний і стрімкий розвиток, що в ньому виникають нові форми правовідносин, які натепер неповністю досліджені та недостатньо врегульовані ані в міжнародному, ані в національному праві.

Також необхідно зауважити, що кіберпростір має два умовні рівні: фізичний (це кабель, волокно, сервери, комп'ютери) [4] та віртуальний (тобто інформаційний). Вплив може здійснюватися на кожному з цих рівнів, а особливістю є те, що вплив на один із рівнів тягне настання наслідків на іншому.

Кіберпростір зручно використовувати не тільки для комунікації та швидкого обміну інформацією, а й для заподіяння шкоди користувачам кіберпростору. У цьому полягає ще одна його особливість, оскільки шкода, заподіяна в кіберпросторі, може бути прямою чи опосередкованою та впливати не тільки на користувачів усередині мережі, а й на зовнішні фізичні об'єкти, які пов'язані з мережею.

Серед основних загроз національним кіберпросторам більшість країн визначають такі:

- кібершпигунство та військові дії, які здійснюються за підтримки або з відома держави. Усі технологічно розвинені держави й корпорації стають об'єктом кібершпигунства, яке має на меті заволодіння державними або промисловими таємницями, персональними даними або іншою цінною інформацією;
- використання Інтернету в терористичних цілях. Терористичні угруповання використовують Інтернет з метою пропаганди, вербування прихильників;
- кіберзлочинність: викрадення персональних даних і відмивання коштів, отриманих незаконним шляхом. Зловмисники продають інформацію про номери банківських карток, паролі та шкідливе ПЗ [5].

Але необхідно також зазначити, що з кіберпростором пов'язані ще такі порушення закону, як інтернет-злочини: порушення прав інтелектуальної власності (піратство), розповсюдження дитячої порнографії, інтернет-шахрайство тощо, які не належать до питань забезпечення кібербезпеки держави, регулюються Конвенцією про кіберзлочинність і становлять окрему сферу суспільних відносин.

Серед нових видів загроз, що виникають у кіберпросторі, одними з ключових є кібератаки. Кібератака – це спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні й технологічні засоби та обладнання) і спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних і/або технологічних системах, отримання несанкціо-

нованого доступу до таких ресурсів; порушення безпеки, сталого, надійного і штатного режиму функціонування комунікаційних і/або технологічних систем; використання комунікаційної системи, її ресурсів і засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [6].

Нині варто передбачати можливість використання кібератак у військових цілях, у зв'язку з чим актуальним стає питання здійснення правового регулювання цих відносин, установлення певних правил поведінки для складників сектору безпеки й оборони.

Отже, кіберпростір – це середовище, яке існує віртуально, але включає у свою структуру об'єкти зовнішнього світу, зазвичай комп'ютери, що підключені до спільної мережі (у більшості випадків мається на увазі мережа інтернет). Дії, які відбуваються в кіберпросторі, можуть впливати на об'єкти зовнішнього матеріального світу. Оскільки всередині віртуального простору не існує певних визначених кордонів, а маніпуляції можливо здійснювати з будь-якого куточку світу, кіберпростір несе не тільки переваги швидкого обміну інформацією, а й новий вид загроз. Кібератаки є одним із найбільш розповсюджених видів заподіяння шкоди в кіберпросторі. Сучасного правового регулювання недостатньо для врегулювання всіх нових відносин, які існують у кіберпросторі, але водночас посилення кількості й сили кібератак змушує уряди різних держав шукати шляхи правового визначення цих понять і заходів відповідного реагування.

Щодо кібероборони. Закон України «Про оборону України» від 06.12.1991 закріплює визначення оборони України як системи політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних, інших заходів держави щодо підготовки до збройного захисту і її захист у разі збройної агресії або збройного конфлікту.

Поняття кібероборони майже тотожне визначенню оборони, крім декількох відмінностей: визначення кібероборони як сукупності, а оборони як системи заходів. Академічний тлумачний словник визначає систему як порядок, зумовлений правильним, планомірним розташуванням і взаємним зв'язком частин чого-небудь [7]. Разом із тим сукупністю є неподільна єдність чого-небудь; загальна кількість, сума чогось [8]. Якщо ми говоримо про заходи, спрямовані на забезпечення оборони держави, більш удалим терміном у цьому випадку є застосування терміна «система», оскільки заходи мають плануватися та здійснюватися у своїй єдності. Сукупність є занадто вузьким терміном у цьому випадку.

Стаття 3 Закону України «Про оборону України» встановлює, що підготовка держави до оборони в мирний час включає таке:

захист інформаційного простору України та її входження у світовий інформаційний простір, створення розвинутої інфраструктури в інформаційній сфері;

здійснення заходів з кібероборони (активного кіберзахисту) для захисту суверенітету держави й забезпечення її обороноспроможності, запобігання збройному конфлікту й відсічі збройній агресії.

Необхідно зазначити, що статтю 3 доповнено новим абзацом щодо здійснення заходів кібероборони згідно із Законом України «Про основні засади забезпечення кібербезпеки України» від 05.20.2017.

Законом України «Про основні засади забезпечення кібербезпеки України» встановлено, які органи державної влади входять до національної системи кібербезпеки. Сама ж національна система кібербезпеки визначена як сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного й технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.

Кібероборона спрямована на забезпечення захисту суверенітету й обороноспроможності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії.

Тобто оборонні заходи входять до заходів забезпечення кібербезпеки, а саме поняття кіберзахисту є ширшим та охоплює поняття кібероборони.

Цим же Законом далі визначено установи, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, а саме:

– міністерства та інші центральні органи виконавчої влади;

– місцеві державні адміністрації;

– органи місцевого самоврядування;

– правоохоронні, розвідувальні й контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

– Збройні Сили України, інші військові формування, утворені відповідно до законів;

– Національний банк України;

– підприємства, установи та організації, зараховані до об'єктів критичної інфраструктури;

– суб'єкти господарювання, громадяни України й об'єднання громадян, інші особи, які провадять діяльність і/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

До повноважень Міністерства оборони й Генерального штабу Збройних Сил України у сфері кіберзахисту, відповідно до вищезазначеного Закону, зараховано заходи з підготовки держави до *відбиття воєнної агресії в кіберпросторі (кібероборони)* (згідно з компетенцією); здійснення військової співпраці з НАТО й іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; упровадження заходів із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного й воєнного стану.

Отже, Законом України «Про основні засади забезпечення кібербезпеки України» встановлено базовий поділ повноважень між органами державної влади щодо здійснення заходів забезпечення кібербезпеки, а органом, що здійснює кібероборону відповідно до компетентності, визначено Міністерство оборони України й Генеральний штаб Збройних Сил України.

Але ні вищезазначений Закон, ні підзаконні нормативно-правові акти не встановлюють саме момент розмежування, коли під час кібератаки необхідно переходити від заходів кіберзахисту до заходів кібероборони та які саме повноваження має Міністерство оборони України й Генеральний штаб Збройних Сил України для здійснення кібероборони. Тобто не визначено зміст і заходи кібероборони.

Наприклад, у Латвії у 2013 році прийнята Концепція кіберпідрозділів у національних збройних силах (National Armed Forses Cyber Defence Unit (CDU) Concept). Згідно із цією Концепцією, на підрозділ мають покладатися такі функції:

1. Забезпечення підтримки CERT.LV та підрозділів Національних Збройних Сил у кризових і військових ситуаціях з погляду запобігання інформаційно-технологічним інцидентам у сфері безпеки й подолання наслідків, що виникли в кіберпросторі, якщо ресурси в розпорядженні CERT.LV є недостатніми й залучення підрозділу прискорює виконання невідкладних заходів [9].

Отже, можна зробити висновок, що, відповідно до вищезазначеної Концепції, функції Міністерства оборони Латвії отримують повноваження, коли ресурсу органу, відповідального за забезпечення кібербезпеки, не вистачає для відбиття кібератаки.

Водночас у Сполучених Штатах Америки підрозділи з кібероборони функціонують з початку 2000-х років і мають чітко визначені повноваження, а, за останніми новинами, Пентагон розширив повноваження кіберкомандування збройних сил Сполучених Штатів Америки, дозволивши представникам цього відомства здійснювати хакерські рейди на іноземні мережі для запобігання кібератакам. Про це повідомляє видання The New York Times з посиланням на нову стратегію американського кіберкомандування. «Нова стратегія передбачає постійну руйнівну діяльність на межі війни в зарубіжних комп'ютерних мережах», – ідеться в повідомленні [10].

У заяві секретаря РНБО України Олександра Турчинова зазначено: «Сучасна війна неможлива без кіберзахисту і без кібератак. Безумовно, ми розглядаємо, я хочу вам сказати,

що в Національному центрі кібербезпеки (РНБО) одне з питань, які ми не так давно розглядали, – це питання, яке доповідав Генштаб щодо створення кібервійськ у лавах ЗСУ» [11].

Висновки. Сфера правового та законодавчого регулювання відносин у кіберпросторі в Україні лише починає формуватися. Законом України «Про основні засади забезпечення кібербезпеки в Україні» визначено основні, базові поняття в цій сфері. Важливим є те, що цей Закон закріпив повноваження Міністерства оборони України та Генерального штабу Збройних Сил України щодо здійснення заходів з кібероборони. Але питання щодо того, що є актом кібернападу, який можна прирівняти до збройної агресії, є нечітко визначеним навіть на міжнародному рівні. До того ж, згідно з тим самим Законом, нечітким є розмежування повноважень між органами щодо здійснення заходів кіберзахисту. Крім того, необхідно зазначити, що кібероборона є одним зі складників, що входять до заходів забезпечення кібербезпеки.

Основною тенденцією українського законодавства натепер є визначення основних повноважень Міністерства оборони України та Генерального штабу Збройних Сил України, але лише в ролі захисників власних інформаційних та інтернет-ресурсів, тоді як у світі кібервійська збройних сил (military cyber defence) займаються захистом та обороною всього кіберспростору своїх держав.

Але, оскільки нині функцію відбиття воєнної агресії в кіберпросторі (кібероборони) покладено на Збройні Сили України, було б логічно на законодавчому рівні надати визначення й ознаки воєнної агресії в кіберпросторі. Без такої дефініції неможливо буде визначити момент, коли від заходів кіберзахисту необхідно буде переходити до кібероборони. Крім того, необхідно визначити межі, у яких можна здійснювати кібероборону.

Список використаних джерел:

1. Рекомендация ООН об использовании многоязычия и всеобщем доступе к киберпространству от 15 октября 2003 года. URL: http://www.un.org/ru/documents/decl_conv/conventions/multilingualism_recommendation.shtml.

2. Рішення Верховного Суду США Reno versus ACLU / 117 S.Ct 2329, 2334-35 (1997). URL: https://www.law.cornell.edu/supct/html/96-511.ZS.html.

3. The Tallinn Manual 2.0. URL: https://ccdcoe.org/tallinn-manual.html.

4. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ, 2014. URL: http://www.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf.

5. Законодавство та стратегії у сфері кібербезпеки (досвід країн Європейського Союзу та США): інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит Комітету Верховної Ради України. URL: http://euinfocenter.rada.gov.ua/uploads/documents/29129.pdf.

6. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: http://zakon2.rada.gov.ua/laws/show/2163-19.

7. Словник української мови. Академічний тлумачний словник (1970–1980). URL: http://sum.in.ua/s/systema.

8. Словник української мови. Академічний тлумачний словник (1970–1980). URL: http://sum.in.ua/s/sukupnistj.

9. National Armed Forces Cyber Defence Unit (CDU) Concept. URL: http://www.mod.gov.lv/~/media/AM/Par_aizsardzibas_nozari/Plani,%20koncepcijas/cyberzs_April_2013_EN_final.ashx.

10. Інтернет видання Тиждень.ua. URL: http://m.tyzhden.ua/news/215603.

11. Уніан, сайт новин. URL: https://www.unian.ua/politics/2378967-turchinov-v-lavah-zbroynih-sil-ukrajini-bude-stvoreno-kiberviyska.html.