Інформаційна і національна безпека

УДК 342.52

БЄЛЄВЦЕВА В.В., *доктор юридичних наук, с.н.с.,* завідувач Наукової лабораторії правових проблем та відповідальності у сфері цифровізації НДІ інформатики і права НАПрН України.
ORCID: https://orcid.org/0000-0001-5573-3744.

ДО ПИТАННЯ ЗАСТОСУВАННЯ ПРАВОВИХ РЕЖИМІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Анотація. *Статтю присвячено дослідженню правових питань застосування та виокремлення правових режимів забезпечення кібербезпеки України. Окреслені правові основи забезпечення кібербезпеки та ознаки правових режимів у цій сфері. У роботі наведені напрями розробки системи правових режимів забезпечення кібербезпеки .*

Ключові слова: *правовий режим, кібербезпека, кіберправопорушення, злочин.*

Summary. *The article is devoted to the research of legal issues of application and the identification of legal regimes for ensuring cybersecurity of Ukraine. These are the legal framework for cybersecurity and the characteristics of legal regimes in this area. The article contains directions for the development of a system of legal regimes for ensuring cybersecurity.*

Keywords: *legal regime, cybersecurity, cyberoffence, crime.*

Аннотация. *Статья посвящена исследованию правовых вопросов применения и выделению правовых режимов обеспечения кибербезопасности Украины. Указанны правовые основы обеспечения кибербезопасности и признаки правовых режимов в этой сфере. В работе приведены направления разработки системы правовых режимов обеспечения кибербезопасности.*

Ключевые слова: *правовой режим, кибербезопасность, киберправонарушение, преступление.*

Постановка проблеми. У сучасних умовах функціонування світової спільноти у цілому та Української держави зокрема, інформаційні і комунікаційні технології є найважливішою частиною сучасних систем управління у всіх галузях економіки. Розширення сфер застосування інформаційних технологій, як чиннику розвитку економіки та удосконалення функціонування громадських і державних інститутів, одночасно є поштовхом для появи нових глобальних викликів і загроз кібербезпеці. Тому охорона та забезпечення кібербезпеки України, попередження та припинення правопорушень у сфері інформаційних технологій були та залишаються найважливішими завданнями відповідних державних органів і суспільства у цілому.

Так, у Стратегії кібербезпеки України, затвердженій Указом Президента України від 15 березня 2016 року № 96/2016, наголошується, що переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб [1].

У Звіті Голови Національної поліції України про результати роботи відомства у 2019 році відзначається, що в Україні у повному обсязі присутні всі ключові "класичні" кіберзлочини, які вчиняються за допомогою комп'ютерних і телекомунікаційних технологій, кількість яких щороку зростає [2]. Це – розповсюдження комп'ютерних вірусів,

шахрайства з платіжними картками, крадіжки грошей з банківських рахунків, викрадення інформації, онлайн-торгівля наркотиками та зброєю, формування у дітей суїцидальної поведінки. Саме протидія цим злочинам є пріоритетом у діяльності Департаменту кіберполіції в 2020 році. Відповідно до тексту вищенаведеного документу у 2019 році викрито 4263 злочини у сфері кіберзлочинності, у тому числі платіжних систем – 1641; протиправний контент – 332; електронна комерція – 744; кібербезпека – 1494.

При цьому слід зазначити, що під терміном "кіберзлочин (комп'ютерний злочин)" розуміється суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [3].

Результати аналізу наукових публікацій з цієї проблеми підтверджують тезу про те, що дослідники дотримуються різноманітних наукових позицій, і наука поки що не виробила єдиного її розуміння. Взагалі, останнім часом спостерігається тенденція поширення термінів з приставкою "кібер" у міжнародно-політичному дискурсі. Вони, навіть, знайшли своє відображення у стратегічних доктринах не лише держав, але й міжнародних організацій, включаючи НАТО. У зв'язку з цим слід відзначити, що представник США у Центрі кібероборони НАТО К. Гірз у своїх працях зазначав, що термін "кібер" використовується стосовно комп'ютерів, інформаційних мереж та цифрової інформації [4, p. 21]. Також слід зауважити, що основою матеріалу, викладеного у даній статті, є аналіз чинного українського законодавства з питань, які стосуються предмету дослідження, а також наукові напрацювання таких вчених, як: Баранов О., Бєляков К., Брижко В., Довгань О., Доронін І., Коваленко Н., Пилипчук В., Рубан В., Тарасюк А., Ткачук Т., Фурашев В. та ін.

Метою статті є визначення особливостей правових режимів забезпечення кібербезпеки в Україні.

Виклад основного матеріалу. На сьогоднішній день, основним документом, що регулює питання міжнародної співпраці щодо протидії кіберправопорушенням, є Конвенція про кіберзлочинність. У даному документі сформульовані принципи щодо забезпечення заходів боротьби з кіберправопорушеннями на національному і міжнародному рівнях. Міжнародна співпраця сприяє вирішенню питань відносно видачі осіб, які вчинили протиправні дії у кіберпросторі, загальних принципів взаємної допомоги щодо правил відправлення інформації, запитів про взаємну допомогу, конфіденційність і забезпечення збереження інформації, транскордонного доступу до неї тощо [5]. Відповідно до даної Конвенції, видача осіб, іншій стороні, можлива за наступні види вчинених кіберправопорушень:

- протизаконний доступ,
- неправомірне перехоплення,
- дія на дані і функціонування системи,
- протизаконне використання пристроїв,
- фальсифікація і шахрайство з використанням комп'ютерних технологій,
- правопорушення, пов'язані з дитячою порнографією,
- порушення авторських і суміжних прав.

Також допускається видача осіб іншим державам, у разі замаху, співучасті або підбурювання до вчинення вищевказаних правопорушень. При цьому, видача осіб, які вчинили правопорушення, можлива за наявності у двох сторін передбаченого покарання у вигляді позбавлення волі на максимальний термін не менше одного року.

Не менш важливим документом, є вище згадувана Стратегія кібербезпеки України

від 15 березня 2016 р. [1]. Отже, метою даної Стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Основу національної системи кібербезпеки України становитимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи.

Слід відзначити, що й до теперішнього часу національні законодавства країн світу зазнали істотні зміни, викликані появою кіберзлочинності та необхідністю вироблення ефективних заходів боротьби з нею. Ці зміни відбувалися паралельно з ухваленням міжнародних документів у сфері боротьби з кіберправопорушеннями. Проте, усі зміни у національних законодавствах держав світу, навіть якщо вони були обумовлені ухваленням будь-якого міжнародного документа, прийняті, розвивалися і змінювалися "автономно". Одні держави вважали за потрібне внести зміни до кримінальних кодексів, інші – ухвалити спеціальні закони, спрямовані на боротьбу з кіберправопорушеннями.

Взагалі, національні законодавства держав світу з питань боротьби з кіберправопорушеннями вельми різноманітні та досить суперечливі. Відсутність одноманітності в національному законодавстві держав світу навіть у межах одного регіону – наприклад, Європи, істотно гальмує розвиток методів ефективної боротьби з кіберправопорушеннями – явищем, для якого не існує державних кордонів. Проте, в деяких державах – наприклад, у США, Італії, Німеччини, – законодавство про кіберправопорушення досить правильно сконструйоване та ефективно застосовується на практиці. Досвід цих держав міг би зіграти позитивну роль і у виробленні міжнародної стратегії, і в реформуванні законодавства з питань боротьби з кіберправопорушеннями в Україні.

Також слід відзначити, що суттєвими проблемами негативної тенденції зростання кількості правопорушень у кіберпросторі є недостатні наукові засади протидії таким правопорушенням та недостатня розробленість нормативно-правової бази у цій сфері. При цьому слід зазначити, що дослідженням різних аспектів забезпечення кібербезпеки України займаються науковці НДІ інформатики і права НАПрН України.

Так, Довгань О.Д. та Тарасюк А.В. у своїх наукових дослідженнях зазначають, що формування та реалізація державної політики щодо запобігання та протидії кіберзлочинності – це процеси, що відбуваються в рамках Національної системи кібербезпеки, які можна розглянути через організаційно-правовий, організаційно-технічний та правоохоронний аспекти [6, с. 95-97].

На наш погляд, одним з інструментів забезпечення кібербезпеки можуть стати правові режими, оскільки інститут правових режимів у сфері кібербезпеки більш поширений, ніж у будь-якій іншій сфері соціально-політичного життя. Частина з них пронизує собою сферу кібербезпеки в цілому, лише конкретизуючись відносно специфіки її окремих складових і суб'єктів забезпечення, інша частина поширюється лише на окремі державні структури.

Схожу думку висловлює у своїх наукових працях Коваленко Н.В., зауважуючи, що кіберпростір на сьогоднішній день відіграє важливу роль у забезпеченні нормального функціонування держав світу й суспільства в цілому. Тому необхідність протидії кіберзагрозам, що можуть зашкодити національній безпеці України, потребує створення власної дієвої системи інформаційної безпеки. Належно розроблена та втілена в життя категорія правового режиму кіберпростору могла б усунути надмірну розшарованість правового регулювання, більш чітко та послідовно визначити суб'єктів досліджуваних правовідносин та порядок їх взаємодії, юридичні гарантії забезпечення прав людини,

форми, методи діяльності контролюючих суб'єктів, заходи юридичної відповідальності. З позитивних моментів у правовому регулюванні є міжнародне співробітництво у сфері кібернетичної безпеки, що забезпечується Конвенцією "Про кіберзлочинність", але, на жаль, поки не усунені недоліки національного законодавства, положення цієї Конвенції не зможуть допомогти працювати механізму національної системи захисту від інформаційних загроз [7, с. 99-100].

Отже, правові режими в цілому найбільше відповідають специфіці забезпечення системи кібербезпеки як більш-менш цілісному утворенню, що виділяється усередині системи інформаційної безпеки. Крім того, ці режими, як правило, беруть свої витоки зсередини цієї сфери і зазвичай поширюють свою дію на інші сфери інформаційної безпеки.

У цьому сенсі, по-перше, слід зазначити, що правові основи забезпечення кібербезпеки України на сьогодні складають міжнародні акти (Конвенція Ради Європи про кіберзлочинність, Угода про асоціацію між Україною та Європейським Союзом, у якій передбачено, що сторони Угоди співробітничають, у тому числі, і з питань протидії кіберзлочинності) та нормативно-правові акти національного законодавства (Стратегія кібербезпеки України, Указ Президента України "Про загрози кібербезпеці держави та невідкладні заходи з їх реалізації", Закон України "Про основні засади забезпечення кібербезпеки України", Закон України "Про захист інформації в інформаційно-телекомунікаційних системах"; постанова Кабінету Міністрів України "Про затвердження правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах"; нормативні документи системи технічного захисту інформації "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" та "Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу"; Наказ Адміністрації Держспецзв'язку України "Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації"; Наказ Адміністрації Держспецзв'язку України "Про затвердження Положення про державну експертизу в сфері технічного захисту інформації"; Наказ Адміністрації Держспецзв'язку України "Про затвердження Положення про державну експертизу в сфері криптографічного захисту інформації" тощо).

По-друге, проаналізувавши вимоги та правила функціонування кіберпростору, визначені у нормативно-правових актах України, можна виокремити ознаки правових режимів забезпечення кібербезпеки, зокрема:

– сфера їх застосування – вони встановлюються у сфері діяльності публічної влади у зв'язку з виконанням органами державної влади своїх обов'язків забезпечити кібербезпеку, охорону, захист;

– розпорядження, режимні правила, що складаються із заборонних та зобов'язальних правових норм, що обмежують загальну правосуб'єктність фізичних і юридичних осіб;

– для правового режиму забезпечення кібербезпеки характерне покладання на державні органи, посадовців, організації, підприємства, громадян обов'язку діяти в певному напрямі для досягнення тієї або іншої мети для забезпечення кібербезпеки;

– обов'язковими суб'єктами правових режимів є компетентні органи публічної влади;

– більшість правових норм, що становлять основу таких режимів, можуть бути реалізовані тільки через правозастосування, шляхом видання індивідуальних правозастосовних актів;

– при регулюванні правовідносин, що виникають між невладними суб'єктами і публічною владою з приводу дотримання режимних правил, застосовується правовий метод впливу;

– порушення правил режиму спричиняє за собою заходи юридичної відповідальності.

Правовий режим забезпечення кібербезпеки у широкому сенсі можна визначити наступним чином – це загальний режим діяльності органів сектору безпеки щодо реалізації покладених на них повноважень.

Правовий режим забезпечення кібербезпеки у вузькому сенсі – це сукупність норм та правил поведінки, діяльності громадян, фізичних та юридичних осіб, що закріплені у нормативно-правових актах, порядок реалізації ними прав і законних інтересів у певних ситуаціях, спрямований на забезпечення кібербезпеки спеціально створюваними з цією метою органами, підрозділами і службами компетентних органівє

Висновки.

Узагальнюючи викладене, можна стверджувати, що особливими ознаками правових режимів забезпечення кібербезпеки є те, що вони:

– встановлюються у діяльності компетентних органів та життєдіяльності осіб та громадян у частині забезпечення функціонування кіберпростору;

– закріплюють, деталізують норми та правила поведінки осіб, громадян, державних органів, суспільних об'єднань, підприємств і установ;

– вводять додаткові обмеження, покладають додаткові обов'язки;

– широко застосовують адміністративні методи впливу;

– вводиться додатковий контроль за дотриманням правил поведінки громадянами, фізичними і юридичними особами, а також органами державного управління;

– порушення норм та правил режиму спричиняє застосування додаткових заходів державного примусу.

При цьому, доцільно звернути увагу на наукові дослідження Довганя О.Д. та Дороніна І.М., де на основі зіставлення результатів аналізу проблем визначення терміна "кібербезпека", та законодавчого визначення терміна "інформаційна безпека" зроблено висновок про те, що кібербезпека – це окремий випадок інформаційної безпеки, поява якого обумовлена використанням комп'ютерних систем та/або телекомунікаційних мереж [8, с. 24-25].

Також, погоджуючись з визначення поняття "кібербезпека" Барановим О.А., зокрема: кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [9], можна сформулювати призначення правових режимів забезпечення кібербезпеки. Таким чином, воно виявляється у наступному: це забезпечення безперебійного функціонування комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації.

Підсумовуючи матеріали даної статті, слід наголосити на тому, що взагалі питання застосування правових режимів у безпековій сфері вже досить давно розглядаються

юристами-науковцями. Звісно, що існують як позитивні, так і негативні аспекти режимного регулювання. Та, на наш погляд, сфера забезпечення кібербезпеки держави є найбільш уразливою з урахуванням сучасних тенденцій розвитку інформаційно-телекомунікаційної сфери, зокрема швидких темпів появи нових загроз. Тому режимно-правове регулювання забезпечення кібербезпеки держави уявляється нами найбільш придатним та дієвим.

У нормативно-правових актах, що регулюють питання забезпечення кібербезпеки України, необхідно визначати вид правового режиму та його носій, підстави введення, суб'єкт, що здійснює режимне управління, режимні заходи і правила діяльності. Оскільки режими в основному пов'язані з обмеженням, примусом, відповідальністю, їх первинне юридичне закріплення проводиться законами, при цьому питома вага урядових і відомчих актів в режимному регулюванні повинна бути зведена до мінімуму.

При розробці засад застосування правових режимів забезпечення кібербезпеки України слід враховувати, що у цій сфері мають місце й загальні, й спеціальні режими.

Узагальнюючи викладене, відзначимо, що розробку системи правових режимів забезпечення кібербезпеки України необхідно проводити у наступних напрямах:

– чіткого визначення предметів і об'єктів системи забезпечення кібербезпеки, її принципів;

– законодавчого відмежування системи правових режимів забезпечення кібербезпеки від інших, близьких за формами і цілями, видів діяльності;

– перегляду системи органів, які здійснюють режимні функції, законодавчого закріплення їх вичерпного переліку та правового статусу, усунення паралелізму і дублювання в роботі;

– розробки механізму взаємодії органів, які формують систему забезпечення кібербезпеки , як між собою, так і з іншими державними органами;

– подальшої деталізації в нормативних актах принципу законності, відповідно до якого застосування правових режимів забезпечення кібербезпеки може здійснюватися лише: а) компетентними органами (посадовими особами); б) у межах їх режимних повноважень; в) з дотриманням процедур (термінів, форм, методів тощо) видачі відповідного дозволу, заборони, припису;

– удосконалення і законодавчого закріплення режимного провадження;

– посилення відповідальності посадових осіб, до повноважень яких відносяться режимні функції;

– удосконалення механізму захисту прав громадянина і людини під час застосування правових режимів забезпечення кібербезпеки тощо.

На нашу думку, запропоновані напрями можуть розглядатись як елементи загальних стандартів, єдині для всієї системи державних органів, що здійснюють режимну діяльність, і які доцільно було б закріпити на законодавчому рівні.

Використана література

1. Стратегія кібербезпеки України: Указ Президента України від 15.03.16 р. № 96/2016. *Офіційний вісник України*. 2016. № 10. С. 39. Ст. 198.

2. Звіт Голови Національної поліції України про результати роботи відомства у 2019 році. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit_2019/zvit-npu-2019.pdf (дата звернення: 16.10.2020).

3. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

4. Geers, K. Strategic Cyber Security. NATO Cooperative Cyber Defence Centre of Excellence, 2011. 169 p.

5. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.05 р. № 2824-IV. *Відомості Верховної Ради України*. 2006. № 5 – 6. Ст. 71.

6. Довгань О.Д., Тарасюк А.В., Глобальна культура кібербезпеки в системі запобігання кіберзлочинності в Україні. *Інформація і право*. № 3(26)/2018. С. 94-103.

7. Коваленко Н.В. Про правовий режим кібербезпеки в Україні. *Актуальні проблеми вітчизняної юриспруденції*. 2016. № 3. С. 96-100.

8. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. – (НДІІП НАПрН України). Київ: Видавничий дім "АртЕк". 2017. 107 с.

9. Баранов О.А. Про тлумачення та визначення поняття "кібербезпека". *Правова інформатика*. № 2(42)/2014. С. 54-62. URL: http://ippi.org.ua/sites/default/files/14boavpk.pdf

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~