УДК 340+35.078.3
DOI https://doi.org/10.32837/pyuv.v0i2(31).576

А. В. Тарасюк
orcid.org/0000-0002-0479-0666
кандидат юридичних наук, старший науковий співробітник,
головний науковий співробітник наукової лабораторії забезпечення
інформаційної та кібернетичної безпеки
Науково-дослідного інституту інформатики і права
Національної академії правових наук України

СИСТЕМНИЙ ПІДХІД У ДОСЛІДЖЕННІ ПРАВОВИХ ОСНОВ КІБЕРБЕЗПЕКИ

Постановка проблеми. Інформатизація і глобалізація життєдіяльності світової спільноти, опанування людством кібернетичного простору, спричинені цим нові загрози й виклики унаочнили важливість правового забезпечення кібербезпеки людини, суспільства й держави, інформаційної безпеки загалом. Як бачимо, сучасна міжнародно-правова термінологія, як-от «глобальні проблеми», «нові виклики й загрози» тощо, повною мірою притаманна й інформаційній сфері та, відповідно, інформаційно-правовій науці. Що стосується нових викликів і загроз у цій сфері, то пов'язані вони насамперед із терористичними проявами (кібертероризмом), кіберзлочинністю із застосуванням новітніх технологій, розповсюдженням у глобальних мережах контенту, спрямованого на інформаційно-психологічний вплив, залякування користувачів, заклики до насильства, розпалювання расової, міжнаціональної, міжконфесійної та іншої ворожнечі, тощо.

Оцінка стану літератури. В основу написання статті покладено теоретичний доробок українських дослідників інформаційного права, зокрема О. Довганя, О. Золотар, В. Фурашева, Т. Ткачука та ін.

Метою дослідження є теоретичне застосування системного підходу до вивчення теоретичних засад правового забезпечення кібербезпеки.

Виклад основного матеріалу. Підхід до наукової розробки проблематики правового забезпечення кібербезпеки людини передбачає насамперед визначення предмета правового регулювання та його специфіки, аналіз положень вітчизняного й міжнародного інформаційного та іншого дотичного законодавства, а також відповідного понятєво-термінологічного апарату. Таким чином, більш широкий підхід, що ґрунтується не лише на власне правовому регулюванні, а й на питаннях правового забезпечення, вбачається оптимальним для досягнення мети цього дослідження. Мається на увазі вивчення не тільки наявної нормативно-правової бази, ненормативних актів державних органів, а й положень документів стратегічного планування, правозастосовної практики тощо.

Отже, під правовим забезпеченням кібернетичної безпеки людини як складової частини правового забезпечення інформаційної безпеки взагалі розуміємо сукупність законодавчих, інших нормативних і ненормативних правових актів державних органів, документів стратегічного планування, правозастосовної практики, які стосуються створення умов для втілення в життя суб'єктивного права людини на кібербезпеку, захищеність від внутрішніх і зовнішніх загроз під час користування кіберпростором. Саме відповідні суспільні відносини і є предметом цього теоретико-правового дослідження, що базується на організаційно-правовій проблематиці, пов'язаній із забезпеченням кібернетичної безпеки людини в динамічних умовах розвитку глобального інформаційного суспільства.

На нашу думку, нині існує чітка взаємозумовленість між прогресом глобального інформаційного суспільства й ефективністю правового забезпечення кібернетичної безпеки особи. Останнє має сьогодні низку істотних недоліків. Це, зокрема: лакуни й суперечності наявної нормативно-правової бази, неповне охоплення нею суспільних відносин, що мають регулюватися й забезпечуватися; серйозні проблеми відповідної правозастосовної практики; низька ефективність наявних правових механізмів протидії викликам і загрозам кібернетичній безпеці тощо.

Слід наголосити на особливій правовій природі суспільних відносин, які виникають у глобальному кіберпросторі у зв'язку із протидією загрозам і викликам кібербезпеці особи, суспільства й держави. Ці відносини становлять вагому частку всього комплексу інформаційних правовідносин, котрі виникають у процесі оперування інформацією (пошуку, отримання, зберігання, передавання, розповсюдження тощо) й регулюються нормами самостійної правової галузі – інформаційним правом.

Вказані відносини мають свої особливості, які вирізняють їх із-поміж інших правовідносин. По-перше, вони виникають, здійснюються і припиняються у процесі обігу інформації. По-друге, вони складаються навколо вельми специфічних об'єктів, а саме: інформації, інформаційних об'єктів і

технологій, кіберпростору, а також феноменів, на які спрямовані інформаційні права й обов'язки.

О. Золотар у своїй докторській дисертації робить справедливий висновок про те, що розуміння інформаційної безпеки людини як правової категорії повинно ґрунтуватися на комплексності її як соціального явища, а також враховувати її внутрішню будову [1, с. 13]. На наше переконання, таке твердження стосується і кібернетичної безпеки.

З урахуванням безумовної потреби дотримання в інформаційних відносинах оптимального балансу інтересів особи, суспільства й держави у цьому дослідженні увага приділяється головному суб'єктові цих відносин – людині в контексті належного правового забезпечення її кібернетичної безпеки. Вбачається важливим дослідити питання інформаційної право- та дієздатності, тобто інформаційно-правової суб'єктності.

У контексті інформаційно-правових відносин щодо протидії викликам і загрозам кібернетичній безпеці людини інформаційну правоздатність можна визначити як установлену, гарантовану й захищену державою можливість або спроможність особи брати участь в інформаційних суспільних відносинах. Тож у сфері кібернетичної безпеки людина набуває певних юридичних прав, а також обов'язків, що передбачають юридичну відповідальність за практичну реалізацію цих прав.

Інформаційну дієздатність як складову частину *інформаційної правосуб'єктності* можна визначити так: спроможність особи своїми діями в інформаційній галузі, у сфері використання кіберпростору набувати прав, брати на себе певні правові обов'язки, а також нести юридичну відповідальність у разі неправомірної поведінки. Нижче детально розглянемо проблематику реалізації людиною своїх законних інформаційних інтересів, прав і свобод за умов сучасних викликів і загроз кібербезпеці.

Що стосується другої важливої складової частини аналізованих правовідносин, пов'язаних із протидією викликам і загрозам кібербезпеці особи, – їх об'єкта, то в контексті цього дослідження його можна визначити так: стан захищеності особи від внутрішніх і зовнішніх загроз в інформаційній сфері при користуванні кіберпростором. Зауважимо, що рівень такої захищеності безпосередньо зумовлює стан забезпечення національних інтересів, істотно впливає на поступ глобального інформаційного суспільства.

Нарешті, ще один складник правовідносин, що розглядаються, – їхній зміст, котрий становлять юридичні права й обов'язки їхніх суб'єктів – особи, суспільства, держави та інших учасників інформаційних правовідносин.

Таким чином, при з'ясуванні правової природи відносин у сфері забезпечення кібернетичної безпеки особи слід комплексно дослідити усі перелічені вище її складники – суб'єкта (людину у глобальному інформаційному просторі, котра потребує належного правового забезпечення своєї безпеки при користуванні кібернетичним простором), об'єкт (стан захищеності особи від внутрішніх і зовнішніх загроз під час використання кіберпростору) та зміст (сукупність прав та обов'язків усіх учасників зазначених суспільних відносин).

Немає жодних сумнівів, що визначальним правовим чинником, генератором розв'язання головних правових проблем у вказаній сфері є система прав і обов'язків. У ній втілюються основні принципи відносин особи та держави, унормовуються правила, стандарти поведінки, які суспільство (через відповідні державні інституції) визнає доцільними, корисними й обов'язковими для своєї нормальної життєдіяльності.

Задля кращого розуміння правової природи правовідносин щодо протидії викликам і загрозам кібербезпеці особи вбачається доцільним звернути увагу на особливості методики їх правового регулювання, яка, виходячи із базових методів правового регулювання, набуває в цьому міжгалузевому правовому інституті своїх специфічних, унікальних способів і прийомів. Інституту правового забезпечення кібернетичної безпеки особи, як і всій галузі інформаційного права, притаманна методика правового регулювання, котра діалектично сполучає імперативний і диспозитивний підходи. Отже, особливості методу інформаційного права полягають у поєднанні способів правового регулювання, які визначені принципами й основними напрямами державної політики у цій сфері.

У своїй «Філософії права» Г.В.Ф. Гегель, погоджуючись із твердженням, що метою держави є щастя громадян, писав: «Це, звісно, правильно: якщо їм зле, якщо їхні особисті цілі не досягаються, якщо вони не бачать, що їх досягнення можливе лише за допомогою держави, то остання стоїть на порцелянових ногах» [2]. У цьому контексті Г.Ф. Шершеневич зазначав, що не можна оминати увагою, пригнічувати особисті інтереси, «але головне в тому, щоби узгодити їх з інтересами цілого» [3].

Відповідно до гегелівської діалектики будь-який розвиток відбувається як перманентний процес: теза (твердження, або покладання) – антитеза (заперечення цього твердження) – синтез (зняття суперечностей, або заперечення заперечення). Як наслідок, у синтезі із тези й антитези виникає якісно новий стан, який, утім, не означає зникнення його вихідних складників. За Гегелем, зняття суперечності, означає також збереження тези й антитези, але в певній більш високій, гармонійній іпостасі.

Ґрунтуючись на цій методології та всебічному аналізу актуального стану взаємин особа – суспільство – держава, спробуємо виявити чинники

внутрішньої суперечливості, ознаки діалектизму, притаманні сучасному інформаційному суспільству. Основними з-поміж них, на нашу думку, є такі: суспільна інертність, неспроможність через певні об'єктивні й суб'єктивні причини належним чином скористатися науково-технічними надбаннями; проблематичність сприйняття особою постійно, лавиноподібно зростаючих обсягів інформації, що зумовлює виникнення певних внутрішніх запобіжників, фільтрів, коли людина визначає важливе й потрібне для себе ще перед сприйняттям інформації, підсвідомо її «фільтруючи»; проблема достовірності інформації, яка циркулює в кіберпросторі, надмірна завантаженість кіберсередовища відвертою дезінформацією, шкідливою чи забороненою інформацією і т. п.; проблеми впровадження інформаційних технологій (нерівномірність, недовіра до, скажімо, електронного урядування замість паперового, яке відточувалося багато віків, тощо); сприйняття новітніх інформаційних технологій у сфері автоматизації як тимчасових через те, що вони постійно вдосконалюються, допрацьовуються, замінюються більш сучасними тощо, тобто не мають усталеної форми; проблема можливості анонімності й водночас ідентифікації суб'єктів кіберпростору за умов глобалізації, транскордонності інформаційного суспільства.

Важливим чинником поступального розвитку інформаційного суспільства є якомога повніше залучення до глобальної інформатизації кожного члена інформаційного суспільства – суб'єкта інформаційних відносин, усвідомлення ним тих можливостей і переваг, які несуть інформаційно-телекомунікаційні технології. Домогтися цього можна тільки в разі забезпечення державою інформаційної, кібернетичної безпеки особи як атрибутивного чинника інформаційного суспільства [4, с. 245]. На жаль, сьогодення свідчить, що рівень такого забезпечення суттєво стримує потенції всебічного прогресу інформаційного суспільства, розвитку і впровадження новітніх інформаційних технологій.

Що стосується конкретних інтересів особи при використанні кібернетичного простору, то це насамперед гарантування доступу до інформації, забезпечення можливості користування величезними можливостями сучасних кібертехнологій, зокрема механізмами електронної демократії (самоврядування, адміністративні, судові та інші послуги тощо). І саме через брак або ж повну відсутність відповідних гарантій і механізмів забезпечення кібербезпеки особи процеси впровадження кібертехнологій і розвиток інформаційного суспільства гальмуються й не отримують належної суспільної підтримки.

Висновки і перспективи подальших досліджень. Слід зазначити, що нині поряд із такими усталеними безпековими іпостасями, як «національна», «державна», «інформаційна», надзвичайно актуалізувалася, сягнула загальнонаціонального рівня проблема кібернетичної безпеки особи. Для з'ясування сутності цього феномену треба розуміти як його статичні, так і динамічні параметри. Статика, яка характеризує певний «стан», не здатна повною мірою охопити й відобразити сутність явища й відповідного поняття.

З огляду на викладене під *кібернетичною безпекою особи розуміємо такий стан її захищеності, який визначається спроможністю особи протистояти внутрішнім і зовнішнім негативним інформаційним впливам, а також здатністю інформаційної держави й інформаційного суспільства забезпечувати її інформаційну безпеку.*

Виникнення й розвиток глобального інформаційного простору, що вбирає в себе усі створені людством інформаційні потоки, актуалізували низку не лише власне технічних питань. Саме існування такого простору породжує також багато проблем морального плану. Постійне зростання вимог до забезпечення інформаційної безпеки особи якраз і зумовлюється глобалізацією й активізацією інформаційних взаємин у сучасному суспільстві [5, с. 184].

Отже, позаяк інформаційна держава об'єктивно стає середовищем людської життєдіяльності, то для забезпечення необхідного рівня її безпеки потрібна ефективна система спеціальних заходів. Задля своєчасного виявлення і знешкодження наявних і потенційних інформаційних загроз, запобігання їм, ліквідації негативних наслідків у разі їх реалізації до комплексу таких заходів мають входити усебічний он-лайн моніторинг електронного врядування. Цілком зрозуміло, що має дотримуватися ієрархія інтересів особи, суспільства й держави, їх оптимальний баланс.

Таким чином, проведений вище аналіз основоположних нормативно-правових актів, ухвалених чи висунутих як проекти у сфері захисту особи, суспільства й держави від загроз і негативних впливів в інформаційному просторі, дає підстави для висновку про засади правового регулювання інформаційної безпеки особи, що склалися нині та за умов систематизації інформаційного законодавства потребують усвідомлення важливості й відповідної уваги до цього інституту інформаційного права з боку законодавчої влади. Підкреслюємо небезпеку при вирішенні глобальних безпекових питань держави й суспільства загалом оминання увагою головного складника інформаційної безпеки – кібернетичної безпеки людини, кожної окремої особи.

Література

1. Золотар О.О. Правові основи інформаційної безпеки людини : автореф. дис. ... докт. юрид. наук : 12.00.07. Харків. 2018. 39 с.
2. Philosophie des Rechts, p. 265,Werke, т. VIII, p. 321.
3. Шершеневич Г.Ф. История философии права. Санкт-Петербург : Издательство «Лань», 2001. С. 512.
4. Ткачук Т.Ю. Інформація з обмеженим доступом на підприємстві: проблеми безпеки та захисту. *Право України*. 2011. № 3. С. 243–252.
5. Ткачук Т.Ю. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право*. 2017. № 10. С. 182–186.

Анотація

Тарасюк А. В. **Системний підхід у дослідженні правових основ кібербезпеки.** – Стаття.

У статті проаналізовано основні тенденції розвитку кіберпростору, а також визначені актуальні проблеми забезпечення кібербезпеки на глобальному та національному рівнях, зокрема у контексті забезпечення безпеки об'єктів критичної інфраструктури, становлення Інтернету речей тощо. За результатами дослідження визначені можливі шляхи вирішення відповідних проблем і підвищення ефективності забезпечення кібербезпеки.

Акцентована увага на актуальності для України питань кіберзахисту цивільних ядерних об'єктів та інших об'єктів критичної інфраструктури. Відсутність конкурентоспроможних вітчизняних рішень на ринку змушує використовувати імпортні аналоги обладнання та програмного забезпечення.

Розроблено систему кібернетичних загроз із зазначенням їхніх джерел і змісту руйнівної дії.

Обґрунтовано, що швидка інформатизація, масштаби потенційних наслідків злочинів у кіберпросторі, недостатня кіберзахищеність об'єктів критичної інфраструктури та ризики, пов'язані з розвитком психологічної Інтернет-залежності, вимагають від національних урядів і міжнародної спільноти серйозної уваги до розвитку систем кібербезпеки на національному та глобальному рівнях. Першочергові кроки в цьому напрямку повинні передбачати розробку необхідної нормативно-правової бази та підвищення ефективності роботи відповідних інституційних структур з урахуванням зарубіжного досвіду в цій сфері.

На глобальному рівні, з огляду на те, що не всі кібератаки підпадають під дію міжнародних механізмів протидії кіберзлочинам, для забезпечення кібербезпеки важливо передбачити зобов'язання держав не вдаватися у кіберпросторі до дій, метою яких є завдання збитків інформаційним системам, процесам і ресурсам іншої держави, критичній інфраструктурі тощо, заради здійснення підриву політичної, економічної й соціальної систем, масованої психологічної обробки населення, що здатні дестабілізувати життєдіяльність суспільства й держави.

Ключові слова: кібербезпека, інформаційна безпека, кіберпростір, кіберзагрози, кіберсистема, критична інфраструктура, Інтернет речей.

Summary

Tarasyuk A. V. **A systematic approach in the study of the legal framework of cybersecurity.** – Article.

The article analyzes the main trends of cyberspace development and identifies related cyber security issues at the global and national levels, in particular in the context of security of critical infrastructure, the emergence of the Internet of Things, and more. The results of the study identified possible ways to solve the problems and increase the effectiveness of cybersecurity.

Emphasis is placed on the relevance of Ukraine to the issues of cyber defense of civilian nuclear facilities and other critical infrastructure. The lack of competitive domestic solutions in the market forces the use of imported analogues of hardware and software.

A system of cyber threats, indicating their sources and the content of the destructive action, has been developed.

It is substantiated that rapid information, the scale of the potential consequences of cybercrime, the lack of cyber security of critical infrastructure and the risks associated with the development of psychological Internet addiction require national governments and the international community to pay serious attention to the development of cybersecurity systems. The first steps in this direction should include the development of the necessary legal framework and the improvement of the efficiency of the work of the respective institutional structures, taking into account foreign experience in this field.

At the global level, given that not all cyber-attacks are subject to existing international cybercrime mechanisms, it is important for cybersecurity to ensure that states are not obliged to act in cyberspace to damage other information systems, processes and resources. the state, critical infrastructure, etc., for the sake of undermining the political, economic and social systems, massive psychological treatment of the population, which are capable of destabilizing the life of society and the state and you.

Key words: cybersecurity, information security, cyberspace, cyber threats, cybersystem, critical infrastructure, internet of things.