УДК 340+35.078.3
DOI https://doi.org/10.32849/2663-5313/2020.7.44

Анатолій Тарасюк,
канд. юрид. наук,
головний науковий співробітник наукової лабораторії забезпечення інформаційної та кібернетичної безпеки
Науково-дослідного інституту інформатики і права
Національної академії правових наук України

МЕТОДОЛОГІЧНІ ПІДХОДИ ДО ВИВЧЕННЯ ПРОБЛЕМИ БЕЗПЕКИ ЛЮДИНИ В КІБЕРПРОСТОРІ

У статті досліджено основні методологічні підходи до вивчення проблем кібернетичної безпеки людини, окреслено тенденції розвитку науки інформаційного права у цій сфері. Проведене дослідження проблем інформаційної безпеки людини дає підстави стверджувати про нагальність питань її правового забезпечення, які потребують всебічного наукового осмислення та формування підходів до їх ефективного розв'язання.

У дослідженні кібернетичної безпеки людини основними методологічними підходами стали загально-філософський, соціологічний, технічний, аксіологічний та правовий підходи. На основі вказаного метрологічного інструментарію визначено, що провідною гіпотезою є залежність, взаємна зумовленість, кореляція ефективності розвитку суспільства в умовах інформатизації й глобалізації та рівня забезпечення кібернетичної безпеки головного споживача всіх набутків сучасних інформаційно-телекомунікаційних технологій – людини, особистості. Факторний аналіз, який є основним методом цього дослідження, базується на вивченні чинників, що у глобальному інформаційному суспільстві впливають на результативність реалізації особою своїх інтересів, становлять для неї небезпеку.

Метою дослідження є визначення концептуальних засад особи в глобалізованому інформаційному суспільстві та стримувальних чинників, пов'язаних із багатоманітністю видів і форм загроз інформаційній безпеці.

Вдосконалено зміст поняття «кібернетична безпека людини», яке запропоновано розуміти як стан її захищеності, що визначається спроможністю особи протистояти внутрішнім і зовнішнім негативним інформаційним впливам, а також здатністю інформаційної держави й інформаційного суспільства забезпечувати її інформаційну безпеку.

Комплексна, міжгалузева природа вказаного правового феномену базується на певній сукупності пов'язаних між собою різногалузевих норм, пріоритет з-поміж яких належить нормам інформаційного права як сполучної ланки й системо утворювального складника. Отже, для розвитку й удосконалення механізму та інструментів інформаційних прав і свобод людини доцільно визнати інститут правового забезпечення кібернетичної безпеки людини самостійним.

Ключові слова: кібернетична безпека, кіберпростір, інформаційне право.

Постановка проблеми. Становлення й еволюція світового інформаційного суспільства, динаміка й характер розвитку глобального кіберпростору зумовили виникнення новітніх викликів і загроз, спрямованих насамперед на людину як найбільш вразливу ланку інформаційних відносин. Тому актуалізувалася проблема формування й удосконалення системи міжнародної кібернетичної безпеки, під якою я розумію такий стан глобального кібернетичного простору, який гарантує дотримання законних прав людини, а також суспільства й держави під час його використання. У зв'язку з цим нагальність теоретико-правового дослідження загроз кібербезпеці людини в контексті правового забезпечення її інформаційної безпеки та розвитку засадничих положень цього складника інформаційного права не викликає сумнівів.

Натепер ми маємо всі симптоми та індикатори загроз, оскільки нам доведеться мати справу з новою біозброєю, зламаною ДНК, і крадіжками генетичної та біометричної інформації. Ми живемо в експоненційні часи, коли інформація подвоюється кожні два роки, коли ми є технологічно незахищеними, адже всіма критичними системами та інфраструктурами керують комп'ютери.

Цікавою є думка керівника відділу інновацій NASA О. Хатамле про експоненційний розвиток технологій. Він зазначає, що якщо просто подивитися на обчислювальну

потужність, яка буде доступна десь до 2030 року, то до того часу вона буде еквівалентна одному людському мозку [1]. І справа не тільки в ІТ-проблемах, які пронизують все життя сучасної людини, яка також стикається із соціальними, особистими, фінансовими проблемами, проблемами охорони здоров'я, виробництва і суспільної безпеки, транспорту та енергетики, конфіденційності і прав людини [2].

Аналіз останніх досліджень і публікацій. В основу написання цієї статті покладено наукові та практичні розробки вчених і дослідників інформаційного права та інформаційних технологій, зокрема це Т. Стоньєр, О. Хатамле, М. Кириченко, Т. Ткачук.

Метою статті є теоретичний аналіз методологічних засад дослідження проблем кібернетичної безпеки для подальшого утвердження інформаційного права як самостійної галузі права.

Виклад основного матеріалу. Інформаційна сфера, в тому числі кібернетична безпека, стали визначальним чинником життєдіяльності сучасної світової спільноти та фактично кожної окремої особистості. Це зумовило, крім звичних розробок технічних аспектів проблематики, сплеск філософських, соціологічних, культурологічних, політологічних, економічних, психологічних та інших гуманітарних досліджень [3, с. 245].

В умовах транскордонного глобалізованого інформаційного суспільства наука інформаційного права мусить звернути особливу увагу на формування уявлень на специфіку та значення реалізації інтересів людини в цій сфері. Забезпечення системності в дослідженні кібернетичної безпеки людини можливе за умови врахування певних методологічних підходів до вивчення зазначеного питання.

Загальнофілософський підхід визначає кібернетичну безпеку людини як єдність трьох складників: задоволення інформаційних потреб особи; забезпечення безпеки інформації; забезпечення захисту суб'єктів інформаційних відносин. Відповідно до цього підходу інформаційною безпекою є такий стан інформаційного середовища, який дозволяє об'єктові, який у ній перебуває, зберігати здатність і мати змогу приймати й втілювати рішення відповідно до спрямованої на прогресивний розвиток мети.

В такому разі кібернетична безпека може забезпечуватися комплексом заходів, спрямованих як на забезпечення стану інформаційного середовища, безпечного для об'єкта, його захисту від шкідливих впливів, так і на розвиток здатності об'єкта уникати таких впливів, зокрема й завдяки знанням про їх наявність, виробленню своєрідного інформаційного імунітету. Для забезпечення інформаційної безпеки держава має створити такі умови функціонування інформаційної інфраструктури та суб'єктів інформаційних відносин (насамперед людини), за яких кожна окрема особа, групи людей, владні інститути зможуть приймати й втілювати спрямовані на прогрес усього суспільства управлінські рішення.

З погляду соціально-політичних реалій пошук засобів протидії численним викликам і загрозам у сфері кібернетичної безпеки насамперед потребує об'єднаних зусиль бізнесових структур, політичних інституцій, правоохоронних та інших органів влади, галузевих аналітичних та експертних спільнот. Кібернетична безпекова політика має відповідати актуальним викликам, тобто спиратися на пріоритети розвитку громадянського суспільства, взаємовигідної співпраці. При цьому держава має стати ефективним менеджером і координатором вказаних процесів [4, с. 184]. Для вироблення та втілення в життя науково-обґрунтованої, системної безпекової політики в інформаційній сфері нині наявні всі передумови.

Багатоаспектним є *технічний* підхід до проблематики кібернетичної безпеки. Це, зокрема, забезпечення безпеки сайтів: атестація, ліцензування й сертифікація об'єктів інформатизації; захист серверів; застосування криптографічних методик і засобів захисту даних у мережах; ідентифікація й аутентифікація користувачів тощо.

Соціологічний підхід щодо кібернетичної безпеки спостерігається в розвитку соціології інформатики – одного з сучасних напрямів науки про суспільство.

Аксіологічний підхід є філософським вченням про природу цінностей, їхню роль у реальному житті та про структуру ціннісного світу, тобто про взаємозалежність різних цінностей, їхні зв'язки із соціальними, культурними чинниками та структурою людської особистості. Базовою категорією аксіології є цінність – особистісне, соціальне й культурне значення певних явищ дійсності. Головне завдання аксіології, її основна ідея – визначення місця цінності в загальній тканині буття, її співвідношення з явищами дійсності, виявлення ролі, яку відіграють певні цінності в людському житті.

При цьому об'єктивність наукового знання й ціннісні судження не повинні суперечити одне одному, оскільки пізнання людини й соціуму не можливе без урахування суб'єктної й суб'єктивної природи людських взаємин, особистісних і суспільних ціннос-

тей, пріоритетів та ідеалів, намірів і прагнень.

Для вироблення нової ціннісної моделі при формуванні інформаційної картини світу потрібна трансформація уявлень про сутність нинішнього інформаційного етапу розвитку людства та ролі особистості в цей період. Ця картина світу має бути усвідомлена не лише об'єктивно, виходячи із характеристик і властивостей новітніх інформаційних технологій, а і з позицій їхньої особистісної та суспільної цінності, тобто відповідності вказаних технологій соціальній природі людини, їх корисності чи шкідливості, безпечності, здатності задовольняти інтереси людини.

Нині термін «інформація» і в науці, й у широкому вжитку може набувати найрізноманітніших значень. За влучним висловом Т. Стоуньєра, інформаційне суспільство все ще не дійшло єдиної думки про те, що таке інформація [5, с. 259]. Втім, не викликає сумнівів міждисциплінарний характер цього поняття, яке застосовується практично в усіх галузях сучасних природничих і соціальних, технічних і гуманітарних, теоретичних і прикладних наук.

З-поміж численних підходів до розуміння інформації в контексті її цінності для інформаційного суспільства можна виокремити три провідних. По-перше, це так званий антропно-комунікативний підхід, тобто тлумачення інформації у сфері спілкування як засобу загальнонаукового усвідомлення міжлюдських соціальних зв'язків і відносин. Другий (функціональний) підхід визначає інформацію як пов'язану з упорядкуванням взаємодій властивість самоорганізуючих систем. Атрибутивний підхід розглядає інформацію як гетерогенність розподілу матерії та енергії – показник такої властивості всіх матеріальних систем.

За таких підходів до тлумачення інформації вже з її поняття випливає можливість порушень інформаційної (кібернетичної) безпеки, тобто інформаційних ризиків. Інформація, яка охоплює всі сфери життєдіяльності суспільства, створює умови інформаційної нерівності, коли вона розподіляється серед соціально-статусних, ресурсних і матеріальних чинників. Така нерівність здебільшого зумовлює виникнення інформаційних ризиків, порушення інформаційної безпеки. Це, зокрема, стосується негативних впливів окремих інформаційних ресурсів маніпулятивного характеру, вторгнення в особистісний інформаційний простір, кібернетичної злочинності та інших порушень інформаційних прав людини. Таким чином, інформаційна безпека людини, суспільства й держави в усіх її аспектах є найважливішою світовою цінністю інформаційної епохи.

Наведені вище міркування стосовно інформаційної картини світу, застосування міждисциплінарної методології як підґрунтя вивчення проблем інформаційної безпеки втрачають сенс без з'ясування «локації» людини в цьому «живописі». Осягнення місця особи у глобальному інформаційному просторі сучасного суспільства пов'язане зі з'ясуванням сутності здатної до критичного мислення людини інформаційної епохи, яка включена у глобальні інформаційні комунікації в філософському та соціальному сенсі.

Важливість такого осягнення важко переоцінити, оскільки це дає змогу виявити нові системні відносини, які виникають в інформаційну епоху у двоєдності людина – суспільство, нові властивості як людини, так і соціуму. Що ж стосується *правових* аспектів кібернетичної безпеки, то нині мусимо констатувати відсутність у юриспруденції єдиного підходу до визначення вказаного поняття. Більш детально це питання буде розглянуто в наступних параграфах дослідження.

Специфіка предмета (кібернетичної безпеки людини) в рамках науки інформаційного права висуває перед дослідниками низку гносеологічних завдань стосовно методів і прийомів пізнання, оптимальних способів систематизації набутих знань, засадничих принципів правового забезпечення в цій галузі, її понятійно-категоріального апарату, закономірностей розвитку тощо. Вважаю, що в умовах глобального інформаційного суспільства ці та інші методологічні проблеми у сфері правового забезпечення інформаційної безпеки потребують першочергового розв'язання.

Вихідним предметом цього дослідження визначено правове забезпечення кібернетичної безпеки особи в умовах глобального інформаційного суспільства. Специфіка цього предмета, яка впливає на характер, перебіг і результати дослідження, полягає насамперед у значущості суб'єкта інформаційних відносин – особистості, її місці і ролі в розвитку цих відносин. Розкрити умови генезису особи в глобальному інформаційному суспільстві, її унікальність, – ці та інші завдання зумовили особистісно орієнтований та аксіологічний підходи цього дослідження, в рамках якого «особа» і «глобальне інформаційне суспільство» є провідними елементами, які визначають важливість проблематики правового забезпечення кібернетичної безпеки особи, а також такі соціально-правові категорії як інформаційна гігієна, екологія інформації тощо.

У цьому дослідженні провідною гіпотезою є залежність, взаємна зумовленість, кореляція ефективності розвитку суспільства в умовах інформатизації, глобалізації та рівня забезпечення кібернетичної безпеки головного споживача всіх набутків сучасних інформаційно-телекомунікаційних технологій – людини, особистості.

Факторний аналіз, який є основним методом дослідження, базується на вивченні чинників, які у глобальному інформаційному суспільстві впливають на результативність реалізації особою її інтересів, становлять для неї небезпеку. Тому метою дослідження є визначення корелятів потенцій особи в глобалізованому інформаційному суспільстві та стримувальних чинників, пов'язаних із багатоманітністю видів і форм загроз інформаційній безпеці.

Оскільки інформаційне законодавство нині проходить етапи свого генезису та становлення як самостійної галузі національного права, воно ще не має, на мою думку, потужної методологічної бази, розроблених засад інформаційно-правової теорії. Наявні у цій сфері нормативні акти не утворюють повноцінну систему інформаційного законодавства, яка б адекватно регулювала правові відносини в інформаційній сфері.

Що стосується методології, то одним із найважливіших питань є проблема сутності правових норм, яка визначається відповідними правовими принципами, тобто тими втіленими у праві вихідними, «первісними» нормативно-керівними засадами, які зумовлюють його формування, підґрунтя, закономірності суспільного життя, відображені в ньому. На жаль, та система принципів, яка простежується в чинному вітчизняному інформаційному законодавстві, свідчить про відсутність цілісного, дієвого механізму правового регулювання суспільних відносин в інформаційній сфері.

Проведене вивчення базисних положень, тобто принципів регулювання суспільних відносин в інформаційній сфері, в галузі комп'ютерних технологій, захисту інформації та кібербезпеки, а також генеральної мети й головних напрямів правового забезпечення захисту інформації й кібернетичної безпеки, втілених у чинних і проектних документах стратегічного планування, дає змоги дійти певних висновків.

Так, зазначені принципи правового забезпечення інформаційної (кібернетичної) безпеки особи необхідно закріпити як базисні під час визначення національних інтересів і стратегічних пріоритетів у Стратегії національної безпеки України, Доктрині інформаційної безпеки та інших документах стратегічного планування, а не лише в законодавстві.

На мою думку, при виробленні державної політики у сфері забезпечення інформаційної, зокрема й кібернетичної, безпеки особи провідними принципами мають стати такі: визнання людини головним суб'єктом і найвразливішим учасником інформаційних відносин; відповідальність інформаційної держави у сфері інформаційних відносин; відповідність організаційно-правових заходів, які вживаються державою, реальним та потенційним викликам і загрозам; державний контроль за забезпеченням інформаційної (кібернетичної) безпеки особи, а також шляхом застосування суспільних інструментів захисту інформаційних прав і свобод.

Про безперечний міжгалузевий характер інституту правового забезпечення кібернетичної безпеки особи переконливо засвідчив аналіз його специфічних рис. Насамперед це стосується різноманітності матеріальних, духовних, соціальних, політичних, культурних та інших інтересів особистості. Одним із найважливіших людських запитів є рівноправ'я в інформаційній сфері, безпосередні комунікації з органами державної влади й місцевого самоврядування у процесі, скажімо, надання останніми послуг за допомогою комп'ютерних мереж, розвитку електронного документообігу, механізмів та інструментів електронної демократії.

Крім того, про міжгалузевий характер інституту, який розглядається, говорить регулювання ним комплексу правовідносин, механізм реалізації яких заснований на нормах інформаційної, конституційної, цивільної, адміністративної, кримінальної, процесуальної, трудової, фінансової, банківської, податкової та інших галузей права.

Висновки

Таким чином, у цьому дослідженні забезпечення кібернетичної безпеки людини розглядається як самостійний комплексний міжгалузевий інститут інформаційного права. Про комплексність зазначеного інституту свідчать, зокрема, такі його властивості:

1) правовий інститут забезпечення кібернетичної безпеки особи сформований і розвивається на базі матеріальних і процесуальних норм інформаційної, конституційної, цивільної, адміністративної, кримінальної, процесуальної (цивільного процесуальної, кримінально процесуальної), трудової, фінансової, банківської, податкової та інших галузей права, хоча й суміжних, але не однорідних;

2) правове забезпечення кібернетичної безпеки особи в системі галузі інформацій-

ного права можна розглядати як самостійне, базове правове утворення, оскільки воно широко представлене в нормах чинного законодавства;

3) інститут правового забезпечення кібернетичної безпеки особи як складник підгалузі правового забезпечення інформаційної безпеки в системі інформаційного права пов'язаний з іншими інститутами цієї підгалузі, зокрема забезпеченням інформаційної безпеки суспільства й держави;

4) основу змісту інституту правового забезпечення кібернетичної безпеки особи становлять норми зазначених вище неоднорідних правових галузей, які об'єднані спрямованістю на забезпечення безпекових інтересів людини в інформаційній сфері.

Комплексна, міжгалузева природа розглянутого вище правового феномену базується на певній сукупності пов'язаних між собою різногалузевих норм, пріоритет з-поміж яких належить нормам інформаційного права як системо утворювального складника. Отже, для удосконалення механізму та інструментів інформаційних прав і свобод людини доцільно визнати інститут правового забезпечення кібернетичної безпеки людини самостійним.

Список використаних джерел:

1. Хатамле Омар. Що відбувається у світі? *Електронний ресурс «На часі»*. URL: https://nachasi.com/2017/09/08/omar-hatamle/.

2. Кириченко М.О. The impact of digital technologies on the development of human and social capital in the conditions of the digitalized society. *Humanities Studies*. 2019. Випуск 1 (78). С. 108–129, 124–125.

3. Ткачук Т.Ю. Інформація з обмеженим доступом на підприємстві: проблеми безпеки та захисту. *Право України*. 2011. № 3. С. 243–252.

4. Ткачук Т.Ю. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право*. 2017. № 10. С. 182–186.

5. Stonier T. Towards a new theory of information. Volume: 17 issue: 5, Issue published: October 1, 1991 page(s): 257–263.

Anatoliy Tarasyuk. Methodological approaches to studying the problem of human security in cyberspace

The article examines the main methodological approaches to studying the problems of human cyber security. The main trends in the development of information law science in this area are outlined. The study of the problems of human information security gives grounds to assert the urgency of the issues of its legal support, which require a comprehensive scientific understanding and the formation of approaches to their effective solution.

In the study of human cyber security, the main methodological approaches were general philosophical, sociological, technical, axiological and legal approaches. Based on these metrological tools, it is determined that the leading hypothesis is the dependence, interdependence, correlation, efficiency of society in the context of informatization and globalization and the level of cyber security of the main consumer of all achievements of modern information and telecommunications technologies – man, personality.

Factor analysis, which is the main method of this study, is based on the study of factors that in the global information society affect the effectiveness of a person's interests, pose a danger to him. The purpose of this study is to determine the conceptual foundations of the individual in a globalized information society and related to the diversity of types and forms of threats to information security deterrents.

The content of the concept of "human cyber security" has been improved, which is proposed to be understood as a state of security, which is determined by a person's ability to resist internal and external negative information influences, as well as the ability of the information state and information society to ensure information security.

The complex, intersectoral nature of the legal phenomenon considered above is based on a certain set of interconnected multidisciplinary norms, the priority of which belongs to the norms of information law as a link and system of the constituent component. For the development and improvement of the mechanism and instruments of human information rights and freedoms, it is considered absolutely expedient to recognize the institution of legal support of human cyber security as independent.

Key words: cyber security, cyberspace, information law.