УДК 342.9
DOI https://doi.org/10.32782/2524-0374/2021-12/72

ПОЛІВЕКТОРНІСТЬ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ГЛОБАЛІЗАЦІЇ

POLYVECTORITY OF LEGAL PROVISION OF INFORMATION SECURITY IN THE CONDITIONS OF GLOBALIZATION

Онопрієнко С.Г., к.ю.н.,
старший викладач кафедри правового забезпечення
Військовий інститут Київського національного університету імені Тараса Шевченка

Мета статті полягала у тому, щоб визначити сутність полівекторності правового забезпечення інформаційної безпеки в умовах глобалізації.

У статті обґрунтовується, що гібридний характер сучасних війн зумовлює підвищення значущості інформаційної безпеки для збереження сталих суспільних відносин, для забезпечення державного суверенітету та територіальної цілісності, створення сприятливих умов для розвитку громадянського суспільства та держави, реалізації прав і свобод людини та громадянина. Інформаційна безпека як складне соціальне явище постає у багатьох аспектах, серед яких найбільше значення, на нашу думку, мають правовий, технологічний і соціально-психологічний. У правовому аспекті інформаційна безпека є комплексом інформаційно-правових засобів, насамперед правових норм, сукупність яких дозволяє поєднувати теорію і практику правового регулювання, досягаючи його цілей. У технологічному аспекті інформаційна безпека становить сукупність виробничих операцій, які змінюють наявний стан захищеності інтересів людини, суспільства й органів публічної влади в інформаційній сфері, завдяки перетворенню наявних або запровадженню нових способів і методів інформаційної діяльності. У соціально-психологічному аспекті інформаційна безпека має розумітися як сукупність особистісних характеристик індивідуальних суб'єктів інформаційних відносин, що зумовлюють збільшення або зменшення інформаційних ризиків під час вибору ними варіантів поведінки у здійсненні діяльності в інформаційній сфері. Визначено сучасні проблеми, які зумовлюють недосконаліть правового забезпечення інформаційної безпеки.

Проблема забезпечення інформаційної безпеки є загальноправовою проблемою і має вирішуватися засобами всіх галузевих правових наук, у межах функціонування яких мають готуватися пропозиції та рекомендації щодо удосконалення правових актів відповідно до предмету цих наук. У цьому проявляється полівекторність інформаційної безпеки, яку ми розуміємо як різноспрямованість її правового забезпечення, що має охоплювати всі сфери публічної, громадської й індивідуальної діяльності, яким можуть спричинити шкоду/небезпеку інформаційні ризики.

Ключові слова: інформаційна безпека, правове забезпечення, інформаційне право, суспільні відносини, інформаційні ризики, полівекторність.

The purpose of the article was to determine the essence of the multivector nature of legal support for information security in the context of globalization.

The article substantiates that the hybrid nature of modern wars leads to an increase in the importance of information security for the preservation of established social relations, for ensuring state sovereignty and territorial integrity, creating favorable conditions for the development of civil society and the state, for the realization of human and civil rights and freedoms. The author has proved that information security as a complex social phenomenon arises in many aspects, among which the most important, in our opinion, are legal, technological and socio-psychological. In the legal aspect, information security is a complex of information and legal means, primarily legal norms, the totality of which makes it possible to combine the theory and practice of legal regulation, achieving its goals. In the technological aspect, information security is a set of production operations that change the existing state of protection of the interests of a person, society and public authorities in the information sphere, due to the transformation of existing or the introduction of new methods and methods of information activities. In the socio-psychological aspect, information security should be understood as a set of personal characteristics of individual subjects of information relations, which cause an increase or decrease in information risks when choosing options for behavior when carrying out activities in the information sphere. The article identifies modern problems that determine the imperfection of the legal support of information security.

The article determines that the problem of ensuring information security is a general legal problem and should be solved by means of all sectoral legal sciences, within which proposals and recommendations should be prepared for improving legal acts in accordance with the subject of these sciences. This is a manifestation of the multivector nature of information security, which we understand as the multidirectional nature of its legal support, which should cover all spheres of public, social and individual activities that may be damaged / dangerous by information risks.

Key words: information security, legal support, information law, public affairs, information hazards, multi-vector.

Постановка проблеми. Останнім часом для характеристики сучасного рівня розвитку суспільних відносин дедалі частіше використовується абревіатура VUCA (від англійських слів «нестабільність» (volatility), «невизначеність» (uncertainty), «складність» (complexity) та «неоднозначність» (ambiguity)). Вказана конструкція виникла у психології лідерства, згодом була запозичена й активно використовувалася під час підготовки військовослужбовців Сполучених Штатів Америки, а сьогодні активно входить у термінологічні апарати наук, які вивчають поведінку людей у соціумі. Сфера права не є винятком, оскільки нестабільність, невизначеність, складність і неоднозначність соціальних процесів не може не впливати на правове регулювання, знижуючи його якість і не дозволяючи досягати цілей, поставлених законотворцем.

Вказане зумовлює необхідність визначення принципів і закономірностей правового забезпечення в умовах світу, який щоденно змінюється. Особливо важливим це є для особливо динамічної сфери інформаційних правовідносин, вплив на котру справляють не лише соціальні процеси, але й нові інформаційні технології, використання яких дозволяє усвідомлювати дедалі нові й нові проблеми.

Мета статті – визначити сутність полівекторності правового забезпечення інформаційної безпеки в умовах глобалізації.

Аналіз останніх публікацій і досліджень. Питання розвитку законодавства про інформаційну безпеку розглядали у своїх роботах такі науковці, як І. Арістова, К. Бєляков, О. Довгань, О. Золотар, Р. Калюжний, Б. Кормич, А. Марущак, О. Олійник, Є. Скулиш, В. Цимбалюк та інші науковці. Водночас складність і багатоплановість проблем розвитку правового забезпечення інформаційної безпеки зумовлює необхідність наукових розвідок за цим напрямом.

Виклад основного матеріалу. Гібридний характер сучасних війн зумовлює підвищення значущості інформаційної безпеки для збереження сталих суспільних відносин, для забезпечення державного суверенітету та територіальної цілісності, створення сприятливих умов для розвитку громадянського суспільства та держави,

реалізації прав і свобод людини та громадянина. Інформаційна безпека як складне соціальне явище постає у багатьох аспектах, серед яких найбільше значення, на нашу думку, мають правовий, технологічний і соціально-психологічний. У правовому аспекті інформаційна безпека є комплексом інформаційно-правових засобів, насамперед правових норм, сукупність яких дозволяє поєднувати теорію і практику правового регулювання, досягаючи його цілей. У технологічному аспекті інформаційна безпека становить сукупність виробничих операцій, котрі змінюють наявний стан захищеності інтересів людини, суспільства й органів публічної влади в інформаційній сфері, завдяки перетворенню наявних або запровадження нових способів і методів інформаційної діяльності. У соціально-психологічному аспекті інформаційна безпека має розумітися як сукупність особистісних характеристик індивідуальних суб'єктів інформаційних відносин, які зумовлюють збільшення або зменшення інформаційних ризиків під час вибору ними варіантів поведінки у здійсненні діяльності в інформаційній сфері.

Як справедливо вказує В. Роллер, агресія Російської Федерації продовжується з різною інтенсивністю та в різному операційному середовищі. Нарівні із застосуванням звичайного кінетичного озброєння під час ведення бойових дій, відзначається інтенсивне використання інформаційно-комунікаційних технологій для досягнення військової мети. За 2019 р. в Україні зафіксовано до одного мільйона кіберзагроз, а лише за перше півріччя 2020 р. локалізовано 356 кібератак на об'єкти критичної інфраструктури держави. Внаслідок втручання у роботу інформаційно-комунікаційних систем, що забезпечують функціонування частин і підрозділів ЗСУ, може бути нанесена значна шкода як економічного характеру, так і військового (виведення з ладу високотехнологічного озброєння та техніки у частині програмного забезпечення унеможливлює його застосування в районі Операції об'єднаних сил за призначенням, що ставить під загрозу виконання поставлених завдань). Стратегічний напрям розвитку держави з метою вступу до Європейського Союзу, прагнення України стати членом Північноатлантичного Альянсу, задекларованe у Конституції України та визначене в основних нормативно-правових актах вищого рівня, передбачає досягнення відповідного рівня взаємосумісності з підрозділами країн-членів НАТО, у тому числі й у питаннях кібероборони. Порівняльний аналіз правового забезпечення заходів кібероборони в державах-членах НАТО й України свідчить про необхідність удосконалення вітчизняного законодавства та приведення його у відповідність до принципів і процедур, визначених у стратегічних та оперативних документах НАТО: Allied Joint Doctrine for Cyberspace Operations; Allied Joint Doctrine for 14 Communication and Information Systems; Allied Joint Doctrine for Electronic Warfare; Allied Joint Doctrine for Information Operations та ін. [1, с. 13–14]. З урахуванням наявних проблем 26 серпня 2021 р. було затверджено нову Стратегію кібербезпеки України, яка враховує попередній досвід і проблеми, стан кібербезпекового середовища на національному та міжнародному рівні, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав – членів ЄС і держав – членів НАТО. Передбачається, що ефективність реалізації Стратегії буде визначатися через постійний моніторинг її виконання та спиратися на чітку систему індикаторів стану кібербезпеки, які буде розроблено протягом першого року реалізації Стратегії. Індикатори мають визначати прогрес, якого досягли суб'єкти забезпечення кібербезпеки у реалізації Стратегії з таких питань, як: виконання стратегічних завдань у межах цілей, визначених Стратегією (за кожним завданням); досягнення стратегічних цілей, визначених Стратегією (за кожною ціллю); рівень впливу заходів, що здійснюються у межах Стратегії, на національну систему кібербезпеки та цифрову трансформацію держави. Упровадження індикаторів стану кібербезпеки забезпечить покращення процесу моніторингу виконання Стратегії у реальному часі з використанням сучасних вебресурсів (онлайн-платформ), прозорість вжитих заходів для суспільства і держави. Посилення впливу національної системи кібербезпеки на суспільний розвиток буде визначатися за такими критеріями, як: рівень довіри населення до держави щодо безпечності кіберпростору; формування безпечного інформаційного суспільства, у якому до заходів кібербезпеки, крім державних інституцій, залучені приватні суб'єкти та громадяни; рівень захищеності національних інтересів у сфері кібербезпеки (як приклад, рівень впливу на розвиток ситуації, пов'язаної з агресією Російської Федерації проти України). За допомогою розгалуженої системи індикаторів буде визначатися стан досягнення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства таі держави. Система індикаторів буде включати базові індикатори стану кібербезпеки, індикатори розвитку національної системи кібербезпеки й індикатори стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, що дасть змогу комплексно оцінювати результативність та ефективність реалізації Стратегії [2], однак, незважаючи на наявність достатньої кількості програмних документів у сфері інформаційної безпеки загалом і кібербезпеки як однієї з її складових частин зокрема, ситуація із реальним їх забезпеченням залишається незадовільною. Значна частина факторів, котрі зумовлюють проблеми із досягненням цілей режиму інформаційної безпеки, мають саме правовий характер.

Як справедливо зауважує О. Панченко, сьогодні відсутня чітко виражена організована система вироблення та реалізації єдиної державної політики у сфері забезпечення інформаційної безпеки, яка визначає пріоритети розвитку єдиного інформаційного простору, що зумовлено такими причинами незадовільного стану у сфері забезпечення інформаційної безпеки, як: безсистемний розвиток законодавства, яке регулює інформаційну сферу; низький рівень правової та інформаційної культури громадян і суспільства загалом; незадовільне фінансування діяльності із забезпечення інформаційної безпеки; недостатній розвиток інформаційних і комунікаційних технологій у сфері державного управління, неготовність органів державної влади до застосування ефективних технологій управління й організації взаємодії із громадянами та суб'єктами господарювання; недостатній рівень підготовки кадрів у сфері створення і використання інформаційних і комунікаційних технологій [3, с. 59]. Погоджуючись з автором, додамо, що частина вказаних проблем має своїми джерелами недостатню увагу до проблем інформаційної безпеки з боку галузевих правових наук.

Безумовно, інформаційне право як комплексна галузь права вивчає відносини, пов'язані з інформаційною безпекою. Водночас, на нашу думку, не існує жодної галузі права, для якої проблема інформаційної безпеки не була би притаманна як власна, нерозривно пов'язана з колом суспільних відносин, які є предметом вказаної галузі. Так, у господарсько-правових відносинах можливий витік інформації суб'єктів господарювання, що становить комерційну таємницю, потребує відповідного правового регулювання додержання інформаційної безпеки (що, до речі, дуже активно здійснюється нині на рівні корпоративного права та договорів про конфедеційність NDA – «Non disclosure agreement»). У кримінально-процесуальних відносинах велика частка аспектів інформаційної безпеки пов'язана з обмеженням розголошення певних відомостей і даних. В адміністративному праві у частині встановлення вимог для кандидатів на заміщення публічних

посад вимоги до інформаційної безпеки мають передбачати наявність у кандидатів низки знань, вмінь і навичок, які гарантують, що вони не піддадуть розголошенню через власну інформаційну некомпетентність відомості, у яких містяться державна та службова таємниця. І такі приклади можна навести для кожної галузі права.

Глобалізація як вироблення універсальних для економік і суспільств різних держав стандартів і правил функціонування соціальних і технологічних процесів надає полівекторності інформаційної безпеки додатковий поштовх для розвитку, оскільки йдеться про транскордонність багатьох виробничих і громадських процесів, коли для їх здійснення поєднуються у віртуальному просторі учасники з різним громадянством, котрі мешкають на територіях різних держав.

Висновки та пропозиції. Вказане свідчить про те, що проблема забезпечення інформаційної безпеки є загальноправовою і має вирішуватися засобами всіх галузевих правових наук, у межах функціонування яких повинні готуватися пропозиції та рекомендації щодо удосконалення правових актів відповідно до предмету цих наук. У цьому проявляється полівекторність інформаційної безпеки, яку ми розуміємо як різноспрямованість її правового забезпечення, що має охоплювати всі сфери публічної, громадської й індивідуальної діяльності, яким можуть спричинити шкоду/небезпеку інформаційні ризики.

ЛІТЕРАТУРА

1. Роллер В.М. Правові засади забезпечення кібероборони в Україні : дис. … докт. філософії : спец. 081. Київ, 2021. 219 с.
2. Стратегія кібербезпеки України. Безпечний кіберпростір – запорука успішного розвитку країни: затверджено Указом Президента України від 26 серпня 2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021/conv#Text.
3. Панченко О.А. Інформаційна безпека в контексті викликів і загроз національній безпеці. *Public Administration and Local Government*. 2020. Issue 2 (45). P. 57–63.