П Р А В О

УДК 342.92
DOI:https://doi.org/10.17721/1728-2217.2022.49.60-62

С. Онопрієнко, канд. юрид. наук
ORCID ID 0000-0002-5524-1798
Київський національний університет імені Тараса Шевченка, Київ, Україна

КЛАСИФІКАЦІЯ ВИДІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ПРАВОВОЇ КАТЕГОРІЇ

На підставі аналізу теоретичних джерел і законодавчої практики запропоновано класифікацію видів інформаційної безпеки. Обґрунтовано розгляд інформаційної безпеки як науково-правової дефініції в широкому та вузькому аспектах. У широкому аспекті інформаційна безпека – це сукупність правових актів, уповноважених ними органів, організації та практики діяльності останніх, поєднання яких породжує механізм забезпечення і захисту інформаційних прав та інтересів людини, соціальних груп, інститутів громадянського суспільства, суб'єктів господарських відносин, органів публічної влади та військових формувань. У вузькому аспекті інформаційна безпека – це стан максимальної захищеності людини, суспільства і держави від інформаційних загроз. Аргументовано, що у широкому аспекті інформаційна безпека може бути класифікована: а) за джерелом походження повноважень щодо здійснення заходів із забезпечення інформаційної безпеки (природні права і свободи людини, Конституція України, закони України, підзаконні правові акти); б) за видами суб'єктів, які забезпечують інформаційну безпеку (людина і громадянин, інститути громадянського суспільства, органи державної влади, органи місцевого самоврядування, військові формування, підприємства, установи та організації всіх форм власності); в) за ступенем обов'язковості здійснення заходів із забезпечення інформаційної безпеки: основна (для спеціально уповноважених органів публічної влади та військових формувань); факультативна (для інших органів публічної влади); делегована (для підприємств, установ та організацій, яким повноваження щодо здійснення заходів інформаційної безпеки делеговано відповідними правовими актами; необов'язкова (для громадян і суб'єктів громадянського суспільства). Визначено, що у вузькому аспекті інформаційна безпека визначається за: а) критерієм суб'єктів, охоплених заходами інформаційної безпеки (інформаційна безпека людини, корпорацій, громадянського суспільства і держави); б) критерієм інформаційних загроз (політична інформаційна безпека, воєнна інформаційна безпека, економічна інформаційна безпека, екологічна інформаційна безпека тощо); в) критерієм досягнутих результатів (досконала і недосконала інформаційна безпека).

Ключові слова: інформаційна безпека, публічна влада, публічне адміністрування, види інформаційної безпеки, суб'єкти інформаційної безпеки, правове забезпечення.

Постановка проблеми. Забезпечення інформаційної безпеки України на сьогодні є найважливішою проблемою, вирішення якої задекларовано як одне з першочергових завдань органів публічної влади. Вирішення цього завдання ускладнюється внаслідок відсутності прозорих і логічних критеріїв розмежування компетенції між суб'єктами забезпечення інформаційної безпеки. У свою чергу, цьому сприяє недостатність теоретико-методологічного підґрунтя, яке визначало б окремі види інформаційної безпеки в системному зв'язку з повноваженнями окремих органів публічного адміністрування, правоохоронних органів, військових формувань. У сукупності це породжує ситуацію, коли забезпеченням інформаційної безпеки займається велика кількість суб'єктів, але відсутність єдиної методологічної бази та критеріїв оцінювання призводить до довільного тлумачення змісту, сутності та результативності здійснюваних заходів. Усі ці фактори слугують підтвердженням актуальності та важливості дослідження видів інформаційної безпеки.

Аналіз останніх досліджень і публікацій. Проблеми інформаційної безпеки розглядали у своїх роботах такі вчені, як: І. Арістова, О. Баранов, К. Бєляков, В. Богуш, О. Довгань, К. Долженко, О. Золотар, Р. Калюжний, Б. Кормич, Ю. Лісовська, А. Марущак, Н. Новицька, О. Олійник, Т. Перун, Є. Скулиш, О. Тихомиров, Т. Ткачук, В. Цимбалюк, В. Фурашев, О. Шевчук та інші науковці. Разом з тим, види інформаційної безпеки ще недостатньо досліджені на теоретичному рівні, що зумовлює актуальність теми цієї статті.

Мета статті полягає в тому, щоб на підставі аналізу теоретичних джерел і законодавчої практики запропонувати класифікацію видів інформаційної безпеки.

Виклад основного матеріалу дослідження. Соціальне призначення інформаційної безпеки в період "гібридних війн" полягає насамперед у створенні, зміцненні та підтримці інформаційного суверенітету як властивості системи публічного управління певної держави забезпечувати додержання верховенства права, законності, прав і свобод людини та громадянина, безперешкодне здійснення інформаційної діяльності органів публічного адміністрування, фізичних та юридичних осіб в інформаційних правовідносинах, що виникають, змінюються та припиняються в межах державних кордонів. Окрім того, соціальне призначення інформаційної безпеки пов'язане з наданням можливості громадянському суспільству в цілому, його інститутам, окремим громадянам реалізовувати своє право на участь у системі публічного управління шляхом доступу до публічної інформації, вільного збирання, накопичення, аналізу, обробки, поширення різноманітних відомостей та даних, а також здійснення громадського нагляду (контролю) без шкоди для національної безпеки. Не менш важливим елементом досліджуваного феномена є те, що за допомогою засобів та інструментів інформаційної безпеки унеможливлюється деструктивний вплив зацікавлених у дестабілізації суспільних відносин суб'єктів, спрямований на формування особистості з бажаними для них якостями, як-то: некритичність у сприйнятті інформації, правовий нігілізм, навіюваність, нестійкість, легкість виникнення панічних настроїв тощо.

Інформаційна безпека як правова і наукова категорія досліджується українськими вченими вже декілька десятиліть, разом з тим складність і багатоплановість цього явища постійно породжує нові конотації цього поняття. Поняття інформаційної безпеки також розглядається в багатьох аспектах, як: "комплекс нормативних документів з усіх аспектів використання засобів обчислювальної техніки для оброблення та зберігання інформації обмеженого доступу; комплекс державних стандартів із документування, супроводження, використання, сертифікаційних випробувань програмних засобів захисту інформації; банк засобів діагностики, лока-

ISSN 1728-3817

лізації і профілактики комп'ютерних вірусів, нові технології захисту інформації з використанням спектральних методів, високонадійні криптографічні методи захисту інформації тощо" [1], як "одна зі сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами" [2, с. 48], як "вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності" [3, с. 48], "захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією України умови існування і розвитку людини, усього суспільства та держави" [4, с. 241]. Розгляд категорії "інформаційна безпека" як вид суспільних відносин, їхній елемент або кінцевий варіант їхньої реалізації дозволив авторам сформулювати велику кількість класифікацій видів досліджуваного феномена. Найбільш повною та аргументованою нам уявляється позиція О. Золотар, яка за об'єктною ознакою виокремлює такі види інформаційної безпеки: людини; юридичних осіб; суспільства; держави (національна інформаційна безпека); міжнародного співтовариства. Відповідно до загроз інформаційній безпеці авторка пропонує розмежовувати внутрішню і зовнішню інформаційну безпеку, причому зміст кожної визначається залежно від того, що чи хто є об'єктом інформаційної безпеки [5, с. 112].

Досліджуючи питання видів інформаційної безпеки, слід насамперед розглянути інформаційну безпеку сфери публічного адміністрування, у якій, власне, і закладається підґрунтя інформаційної безпеки інших суб'єктів суспільних відносин. Відносини, що складаються у сфері публічного адміністрування, спрямовані на забезпечення публічного інтересу. Під публічним інтересом розуміємо сукупність цілей, прагнень, потреб, які виникають у фізичних та юридичних осіб у процесі їхньої діяльності (життєдіяльності), задоволення яких потребує здійснення суб'єктами публічного адміністрування юридично значущих дій. Отже, ті учасники суспільних відносин у сфері публічного адміністрування, які не мають статусу посадових осіб органів державної влади і місцевого самоврядування, можуть бути фізичними особами, представниками громадянського суспільства, суб'єктами господарської діяльності тощо. Для кожного з них реалізація свого публічного інтересу за участю органів публічного адміністрування породжує ситуацію ризику, ситуацію можливого виникнення інформаційної небезпеки. На наш погляд, інформаційна безпека сфери публічного адміністрування є складовою національної інформаційної безпеки, яку можна представити як сукупність інформаційної безпеки законодавчої і судової влади, а також інформаційної безпеки органів публічного адміністрування (як сукупності органів виконавчої влади та органів місцевого самоврядування). Відповідно до специфіки функціонування органів публічного адміністрування, загрози інформаційній безпеці у їхній діяльності можуть мати як зовнішній, так і внутрішній характер.

Інформаційна безпека сфери публічного адміністрування може також бути класифікована за характером ризиків. Якщо ризики мають технологічний характер і стосуються безпеки обладнання та програм, використовують поняття "кібербезпека". У Законі України "Про основні засади забезпечення кібербезпеки України" кібербезпека розуміється як 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 в кіберпросторі [6]. Невдалість вказаного легального визначення значно утруднює його розуміння, оскільки більшість його складових потребує окремого тлумачення. Так само було б доцільно для цілісного сприйняття розмежувати категорію "кібербезпека" з категорією "інформаційна безпека". Кібербезпека є складовою інформаційної безпеки, поряд з особистою та корпоративною інформаційною безпекою.

Слід сказати, що проблеми підвищення рівня інформаційної безпеки надзвичайно важливі в сучасний період реформування системи публічного управління. Вирішення цих проблем потребує використання ряду заходів політичного, економічного, технологічного, соціально-психологічного характеру. Проте саме право має стати тією інтегруючою категорією, яка органічно поєднає різновекторні складові інформаційної безпеки, надасть останній структурований характер, дасть змогу кожному суб'єкту правовідносин у сфері публічного адміністрування розуміти коло своїх прав та обов'язків, а також міру своєї юридичної відповідальності за порушення правових приписів. Вказане потребує вдосконалення як інформаційно-правових актів, так і законодавства у сфері публічного управління, оскільки цінність теоретичних положень може бути втілена у площину правовідносин лише за допомогою відповідних змін у правовому регулюванні. Це має відбуватися шляхом конкретизації обов'язків органів публічної влади в досліджуваній сфері, а також встановлення заходів юридичної відповідальності за невиконання відповідних правових приписів.

Висновки. Інформаційну безпеку як науково-правову дефініцію можна розглядати у двох аспектах: широкому та вузькому. У широкому аспекті інформаційна безпека – це сукупність правових актів, уповноважених ними органів, організації та практики діяльності останніх, поєднання яких породжує механізм забезпечення та захисту інформаційних прав та інтересів людини, соціальних груп, інститутів громадянського суспільства, суб'єктів господарських відносин, органів публічної влади та військових формувань. У вузькому аспекті інформаційна безпека – це стан максимальної захищеності людини, суспільства і держави від інформаційних загроз.

У широкому аспекті інформаційна безпека може бути класифікована за: а) джерелом походження повноважень щодо здійснення заходів із забезпечення інформаційної безпеки (природні права і свободи людини, Конституція України, закони України, підзаконні правові акти); б) видами суб'єктів, які забезпечують інформаційну безпеку (людина і громадянин, інститути громадянського суспільства, органи державної влади, органи місцевого самоврядування, військові формування, підприємства, установи та організації всіх форм власності); в) ступенем обов'язковості здійснення заходів із забезпечення інформаційної безпеки: основна (для спеціально уповноважених органів публічної влади та військових формувань); факультативна (для інших органів публічної влади); делегована (для підприємств, установ та організацій, яким повноваження щодо здійснення заходів інформаційної безпеки делеговано відповідними правовими актами; необов'язкова (для громадян і суб'єктів громадянського суспільства).

У вузькому аспекті інформаційна безпека включає такі види: а) за критерієм суб'єктів, охоплених заходами інформаційної безпеки (інформаційна безпека людини, корпорацій, громадянського суспільства і держави); б) за критерієм інформаційних загроз (політична інформаційна безпека, воєнна інформаційна безпека, економічна інформаційна безпека, екологічна інформаційна безпека тощо); в) за критерієм досягнутих результатів (досконала і недосконала інформаційна безпека).

Напрями подальших наукових досліджень мають включати розмежування компетенції суб'єктів інформаційної безпеки на підставі розмежування їхніх повноважень і закладених у правових актах та статутах цілей діяльності відповідно до виділених видів інформаційної безпеки.

Список використаної літератури

1. Про Концепцію Національної програми інформатизації : Закон України від 4 лютого 1998 р. № 75/98-ВР. URL : https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text (дата звернення 11.02.2020).

2. Литвиненко О. Інформація і безпека. *Нова політика*, 1998. № 1. С. 47–49.

3. Фурашев В.М. Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки. *Інформація і право*, 2012. № 1(4). С.46–56.

4. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України : монографія. Одеса : Юридична література, 2003. 472 с.

5. Золотар О. О. Класифікація інформаційної безпеки. *Інформація і право*, 2011. № 2. С. 109–113.

6. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 11.02.2020).

References

1. On the Concept of the National Informatization Program: Law of Ukraine of February 4, 1998 № 75/98-VR. URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text [in Ukrainian].

5. Litvinenko, O. (1998) Information and security. *New policy,* № 1, p. 47–49. [in Ukrainian].

6. Furashev, V.M. (2012) Issues of legislative definition of the conceptual and categorical apparatus in the field of information security. Information and law, № 1 (4), p.46– 56. [in Ukrainian].

7. Kormich, B.A. (2003) Organizational and legal principles of information security policy of Ukraine: Monograph. Odessa, 472 p. [in Ukrainian].

8. Zolotar, O.O. (2011) Classification of information security. Information and law, № 2, pp. 109–113. [in Ukrainian].

9. On the basic principles of cybersecurity of Ukraine: Law of Ukraine of October 5, 2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

Надійшла до редколегії 04.02.22

S. Onopriienko, PhD of Juridical Sci.
ORCID ID 0000-0002-5524-1798
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

CLASSIFICATION OF THE TYPES OF THE INFORMATION SECURITY AS A LEGAL CATEGORY

The purpose of the article was to propose a classification of types of information security from the analysis of theoretical sources and legislative practice. The article substantiates that information security as a scientific legal definition can be considered in two aspects: broad and narrow. In a broad aspect, information security is a set of legal acts, bodies authorized by them, organization and practice of the latter, the combination of which generates a mechanism for ensuring and protecting the information rights and interests of a person, social groups, civil society institutions, subjects of economic relations, public authorities. and military formations. In a narrow aspect, information security is the state of maximum protection of a person, society and the state from information threats. Arguments are given that, in a broad aspect, information security can be classified: a) by the source of origin of the authority to implement measures to ensure information security (natural human rights and freedoms, the Constitution of Ukraine, laws of Ukraine, by-laws); b) by types of entities providing information security (individual and citizen, civil society institutions, state authorities, local governments, military formations, enterprises, institutions and organizations of all forms of ownership); c) according to the degree of obligation to implement measures to ensure information security: the main one (for specially authorized public authorities and military formations); optional (for other public authorities); delegated (for enterprises, institutions and organizations to which the authority to implement information security measures is delegated by the relevant legal acts; optional (for citizens and civil society entities). The article substantiates that in a narrow aspect, information security includes the following types: a) according to the criterion of subjects covered by information security measures (information security of a person, corporations, civil society and the state); b) according to the criterion of information threats (political information security, military information security, economic information security, environmental information security, etc.); c) according to the criterion of achieved results (perfect and imperfect information security).

Keywords: information security, public authorities, public administration, types of information security, subjects of information security, legal support.