

Інформаційна безпека в контексті національної безпеки: адміністративно-правова характеристика

Надія Петрівна Бортник ¹

| Опубліковано | Секція | УДК |
|--------------|--------|---------|
| 29.12.2023 | Право | 342.951 |

DOI: <http://dx.doi.org/10.5281/zenodo.10516910>

Ліцензовано за умовами Creative Commons BY 4.0 International license

Анотація. Стаття присвячена адміністративно-правовій характеристиці інформаційної безпеки в контексті національної безпеки держави. Звернуто увагу на те, що інформаційна безпека для нашої держави стала актуалізуватись з першими проявами формування інформаційного суспільства і вже тривалий час перебуває на піку такої актуальності. Складові, які охоплює категорія «інформаційна безпека», це передусім, людина, держава та загалом суспільство, які мають бути убезпечені від негативного впливу у сфері інформації.

Наголошено на тому, що сучасний стан світопорядку сьогодні не обмежений різноманітними аспектами, які мають і позитивний, і негативний вплив на інформаційну безпеку, а тому містить багато невирішених наукових і прикладних питань. Особливий аспект інформаційної безпеки в Україні сьогодні пов'язаний з протидією інформаційній війні, інформаційній зброї, які разом з повномасштабним військовим вторгненням використовує країна-агресор, – російська федерація, проти нашої держави.

Зроблено висновок, що в умовах сьогодення цілком логічно розглядати питання інформаційної безпеки на двох рівнях, якими є глобальна інформаційна безпека та національна інформаційна безпека. У цьому контексті вагоме значення має бути надано правовому регулюванню сфери інформаційної безпеки, сутності та специфіці змісту діяльності органів публічної влади щодо забезпечення інформаційної безпеки як складової національної безпеки.

Ключові слова: безпека, національна безпека, інформація, інформаційна безпека, інформатизація, інформаційна війна, інформаційна зброя, протидія загрозам і викликам, кібербезпека.

Information security in the context of national security: administrative and legal characteristics

Abstract. The article is devoted to the administrative and legal characteristics of information security in the context of national security of the state. Attention was drawn to the fact that information security for our country became relevant with the first manifestations of the formation of an information society and has been at the peak of such relevance for a long

¹професор кафедри теорії та історії держави і права факультету морського права Національного університету кораблебудування імені адмірала Макарова, доктор юридичних наук, професор <https://orcid.org/0000-0002-3030-406X>

time. The components covered by the category «information security» are, first of all, a person, the state and society in general, which must be protected from negative influence in the information sphere.

It is emphasized that the current state of the world order today is not limited by various aspects that have both positive and negative effects on information security, and therefore contains many unresolved scientific and applied issues. A special aspect of information security in Ukraine today is related to countering information warfare, information weapons, which, together with a full-scale military invasion, are used by the aggressor country, the Russian Federation, against our state.

It was concluded that in today's conditions it is quite logical to consider the issue of information security at two levels, which are global information security and national information security. In this context, significant importance should be given to the legal regulation of the field of information security, the essence and specificity of the content of the activities of public authorities in ensuring information security as a component of national security.

Keywords: security, national security, information, information security, informatization, information warfare, information weapons, countering threats and challenges, cyber security.

Вступ

Постановка проблеми. Проблематика інформаційної безпеки в контексті забезпечення національної безпеки упродовж останніх десятиліть для нашої держави була досить актуальною. Нового наукового піднесення ця тема набула з огляду на інформаційну війну розпочату країною-агресором – російською федерацією проти України. Водночас, варто зауважити, що сучасний стан світопорядку також не обмежений різноманітними аспектами, які мають і позитивний, і негативний вплив на інформаційну безпеку, а тому містить багато невирішених наукових і прикладних питань.

Стан дослідження проблеми. Вказана тема широко висвітлюється фахівцями у галузі адміністративного та інформаційного права, які зокрема торкаються і безпекових питань у широкому розумінні. З-поміж них особливе зацікавлення становлять праці: В. Авер'янова, О. Андрійко, І. Арістової, О. Баранова, А. Берлача, Ю. Битяка, К. Белякова, В. Білоуса, В. Брижка, В. Гавловського, В. Галунька, М. Гурковського, М. Гуцалюка, С. Єсімова, Р. Калюжного, М. Коваліва, Т. Коломонець, В. Колпакова, А. Комзюка, Б. Кормича, Т. Кравцової, О. Кузьменко, В. Курила, А. Новицького, В. Ліпкана, С. Петкова, О. Рябченко, В. Цимбалюка, М. Швеця, І. Шопіної, Х. Ярмакі та багатьох інших.

Метою статті є адміністративно-правова характеристика інформаційної безпеки в контексті національної безпеки держави.

Результати

Виклад основного матеріалу. Передусім, необхідно зауважити, що нинішнє суспільство, яке прийнято називати інформаційним, вже давно і досить глибоко вкорінилося в наше життя, зробивши нас залежними від такої категорії як інформація. Як зазначає, Н. Уханова, інформація сьогодні перетворилась на важливий економічний, політичний та соціальний ресурс. Сучасний світ, задовольняючи потреби людей в отриманні та переробці інформації, сприяє їхній орієнтації в швидкозмінюваних політичних та соціально-економічних умовах, змушує бути гнучкими у сприйнятті інформації та активними учасниками тих чи інших суспільно-політичних подій [1, с. 91].

З огляду на це, варто підтримати тезу, І. Тацишина, який вважає, що одним з головних пріоритетів побудови України, стала побудова орієнтованого на інтереси

людей безпечного інформаційного суспільства, метою якого є створення і накопичення інформації та знань, вільний доступ, користування і обмін ними [2, с. 46].

Водночас, як слушно зауважує, О. Прудникова, «сучасна інформаційна епоха, яка з проекту перетворилась на реальність, уже виявляє як сильні, так і слабкі свої сторони, проявляється у нових формах і феноменах, породжує небувалі можливості й ризики. Формується єдине інформаційне середовище, яке визначає нову культуру як суспільства в цілому, так і кожної людини окремо. Нинішній етап розвитку цивілізації характеризується тим, що жодна сфера буття людини не може нормально функціонувати і розвиватися без своєчасного й повного забезпечення необхідною інформацією, уміння її швидко, якісно й адекватно сприймати, зберігати, обробляти, використовувати і передавати» [3, с. 5].

Звертаючи увагу на деякі інформаційні виклики сучасності та їх відображення в інформаційному просторі Д. Ланде, висновує, що суспільні виклики щодо інформаційної сфери можуть привести до руйнування або переформатування засад сучасної економіки, зокрема у питаннях, що стосуються авторського та суміжних прав, приватності, екстериторіальності тощо [4, с. 19].

З огляду на це, надзвичайно важливого значення в умовах сьогодення набула категорія «інформаційна безпека», яка на рівні Конституції України, як Основного Закону держави, визнана найважливішою (з-поміж інших) функцією «держави, справою всього Українського народу» [5].

Розкриваючи методологічний аспект безпеки як об'єкта правовідносин в умовах глобального інформаційного суспільства, В. Гурковський, також вважає інформаційну безпеку важливою складовою процесів, спрямованих на задоволення людиною, державами, міжнародним співтовариством потреб та інтересів щодо інформації із застосуванням різноманітних технологій на основі комп'ютерних технічних засобів, у тому числі глобальних засобів електронної телекомунікації. На думку вченого, основними складовими інформаційної безпеки є безпека людини, суспільства, держави, міжнародного співтовариства у сфері інформації [6, с. 73].

Характеризуючи питання інформаційної безпеки варто наголосити на тому, що вона є одним із видів національної безпеки, а отже, будь-які виклики та загрози, що посягають на інформаційну безпеку, безпосередньо впливають на безпеку національну.

У цьому контексті цілком обґрунтованими видаються думки І. Мусієнка, стосовно того, що лише надійна та ефективна система забезпечення національної безпеки може бути гарантом суверенітету і незалежності країни, її стабільного соціально-економічного розвитку й добробуту. Вчений вважає, що національна безпека є динамічним явищем, що розвивається разом зі зміною і ускладненням суспільних відносин, технологій тощо. Це вимагає постійного удосконалення системи її забезпечення, адже будь-які недоліки в ній здатні завдати непоправної шкоди національним інтересам держави [7, с. 76].

Цілком логічними, стосовно вагомості інформації та інформаційних технологій є думки, які висловили, О. Юдін та В. Богуш. Вчені вважають, що «інформаційні технології знаходять усе ширше застосування у таких сферах, як фінансовий обіг і ринок цінних паперів, зв'язок, транспорт, високотехнологічні виробництва (особливо атомні, хімічні тощо), державні системи управління і т. ін. Будь-яка диверсія у наведених сферах життєдіяльності держави й суспільства може призвести до тяжких наслідків, паралізувати як ординарні, так і складні, «високі» системи управління, збройні сили і спеціальні служби, спровокувати руйнівні аварії на екологонебезпечних об'єктах» [8, с. 32].

Вочевидь, в умовах, коли Україна виборює свою незалежність, суверенітет і територіальну цілісність від агресивного і повномасштабного вторгнення російської

федерації, яка з-поміж іншого вдається і до застосування усіх можливих інформаційних загроз, Україна намагається протидіяти цьому, шляхом забезпечення належної інформаційної безпеки.

Вказане, зокрема, прослідковується з низки законодавчих та підзаконних актів, які прийняті в Україні протягом останніх років. Так, п. 4 ст. 3 Закону України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII встановлює, що «державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на інші її напрями» [9].

Важливим кроком на шляху посилення діяльності щодо забезпечення інформаційної безпеки стало введення в дію рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України». Пункт 52 Розділу III «Основні напрями зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки», цього нормативно-правового акта встановив важливість розвитку кібербезпеки, яка займає першочергове місце у забезпечення національної безпеки загалом та інформаційної безпеки держави, зокрема, а основним завданням у цьому процесі є «гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації» [10].

Законом України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року, кібербезпека визначена 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 у кіберпросторі» [11].

Варто погодитись з О. Косіловою, що сьогодні існують певні загрози інформаційній безпеці, які мають міжнародне значення. Такими, на думку вченої, є інформаційний тероризм, комп'ютерна злочинність, інформаційні війни, використання інформаційної зброї, маніпулювання громадською думкою тощо [12, с. 27].

Розглядаючи питання інформаційної безпеки України в умовах глобалізації, О. Косілова, робить висновок, що для нейтралізації та попередження загроз інформаційній безпеці України слід на державному рівні послідовно розробляти та вдосконалювати нормативно-правову базу, підвищувати науковий потенціал у галузі інформатизації, телекомунікації та зв'язку, вдосконалювати систему захисту вітчизняної інформаційної інфраструктури. Необхідно також удосконалювати форми і способи активної протидії інформаційно-психологічним операціям, спрямованим на послаблення обороноздатності країни, моделей превентивного інформаційного впливу, захисту інформаційного суверенітету [12, с. 27].

Досліджуючи інформаційну безпеку та інформаційну культуру в сучасному інформаційному суспільстві, О. Панченко та Л. Панченко формулюють авторський підхід до розуміння інформаційної безпеки, яка, на їх думку, є станом інформаційного середовища, що забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин, безпеку інформації і захист суб'єктів від негативної інформаційної дії [13, с. 34].

Водночас, на основі такого визначення, науковці поділяють загрози інформаційній безпеці на: а) порушення безпеки інформації, тобто загрози об'єктивній складовій інформаційного середовища; б) порушення безпеки об'єкта/суб'єкта захисту внаслідок незадоволення його інформаційних потреб або деструктивних інформаційних дій, тобто загрози суб'єктивній складовій інформаційного середовища [13, с. 34].

Стратегія інформаційної безпеки, яка введена Указом Президента України від 28 грудня 2021 року № 685/2021 розглядає загрози та виклики інформаційній безпеці у двох вимірах: по-перше, через глобальні виклики та загрози та по-друге, через національні виклики та загрози [14].

Глобальними викликами та загрозами у вказаній Стратегії визначено такі:

- збільшення кількості глобальних дезінформаційних кампаній;
- інформаційна політика Російської Федерації – загроза не лише для України, але й для інших демократичних держав;
- соціальні мережі як суб'єкти впливу в інформаційному просторі;
- недостатній рівень медіаграмотності (медіакультури) в умовах стрімкого розвитку цифрових технологій» [14].

Натомість, на рівні національних викликів і загроз визнано:

- інформаційний вплив Російської Федерації як держави-агресора на населення України;
- інформаційне домінування Російської Федерації як держави-агресора на тимчасово окупованих територіях України;
- обмежені можливості реагувати на дезінформаційні кампанії;
- несформованість системи стратегічних комунікацій;
- недосконалість регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів;
- спроби маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції України;
- доступ до інформації на місцевому рівні;
- недостатній рівень інформаційної культури та медіа грамотності в суспільстві для протидії маніпулятивним та інформаційним впливам [14].

Важливим напрямом, спрямованим на забезпечення інформаційної безпеки є наукові розробки цієї тематики та напрацювання, які сприятимуть удосконаленню норм чинного законодавства, що регулює цю сферу. Так, окреслюючи дослідження проблем інформаційної безпеки у юридичній науці, А. Марущак, наголошує на тому, що доречним у цьому контексті видається підхід, відповідно до якого класичні напрями досліджень юридичної науки застосовувалися б до проблем, пов'язаних з інформаційною безпекою. У цьому контексті звернуто увагу на:

- науково-теоретичне обґрунтування доцільності правового регулювання суспільних відносин, що виникають з приводу інформаційної безпеки особи, суспільства, держави;
- визначення основних понять та категорій, які застосовуватимуться для унормування відповідних суспільних процесів;
- наукові розробки щодо повноважень суб'єктів суспільних інформаційно-безпекових відносин, форм і методів їх реалізації;
- дослідження питань юридичної відповідальності за правопорушення у сфері інформаційної безпеки [15, с. 17-18].

Не менш важливою складовою у цьому процесі є підготовка спеціалістів у сфері забезпечення інформаційної безпеки. Стосовно цього, на думку згаданого нами І. Мусієнка, необхідно враховувати принаймні такі аспекти (напрями) формування знань і навичок: а) необхідних для роботи по лінії забезпечення інформаційної безпеки держави; б) необхідних для професійного застосування сучасних інформаційно-комунікативних технологій, методів отримання і аналізу інформації [7, с. 81].

Водночас, Л. Куренда досить справедливо звертає увагу на те, що міжнародне співтовариство визнає, що боротьба та протиборство між країнами на сьогодні

здійснюється переважно з використанням інформаційної зброї, що зумовлює інформаційний характер загроз та небезпек.

У зв'язку з цим міжнародна спільнота термінологічно узгодила інші важливі поняття. Так, під «інформаційною війною» слід розуміти інформаційне протиборство з метою впливу на критично важливі структури противника, зруйнування політичної та соціальної систем, а також для дестабілізації суспільства і державності противної сторони. «Інформаційна зброя», у свою чергу, визначається як комплекс технічних та інших заходів, методів і технологій, спрямованих на встановлення контролю над інформаційними структурами потенційного противника, втручання у роботу його систем управління, інформаційних мереж та комунікацій з метою знищення або модифікації даних, дезінформації, поширення інформації спеціального призначення у системах формування громадської думки і прийняття рішень, а також як сукупність засобів впливу на свідомість і психологічний стан політичних та військових структур, спецслужб і населення для протидії можливим інформаційним впливам іншої сторони [16, с. 38].

Висновки

Отже, підсумовуючи викладене вище можемо констатувати, що інформаційне суспільство, яке практично у багатьох державах світу вийшло зі свого етапу формування та розпочало активний розвиток, разом із значними перевагами внесло і такі небезпечні аспекти як загрози та виклики. Інформація, що стала необхідною для людини, держави і суспільства, за таких обставин зачепила важливі безпекові питання, що зумовило виникнення таких категорій як національна безпека та її складової – інформаційної безпеки.

В умовах сьогодення цілком логічно розглядати питання інформаційної безпеки на двох рівнях, якими є глобальна інформаційна безпека та національна інформаційна безпека. У цьому контексті вагоме значення має бути надано правовому регулюванню сфери інформаційної безпеки, сутності та специфіці змісту діяльності органів публічної влади щодо забезпечення інформаційної безпеки як складової національної безпеки.

Список використаних джерел

1. Уханова Н. С. Інформаційно-психологічна безпека особистості, суспільства та держави. *Правова інформатика*. 2013. № 3(39). С. 91–95.
2. Тацишин І. Б. Національна безпека України та її складові елементи. *Правова інформатика*. 2008. № 4 (20). С. 46–49.
3. Прудникова О. В. Інформаційна культура: концептуальні засади та світоглядний сенс: монографія. Х.: Право, 2015. 352 с.
4. Ланде Д. В. Деякі інформаційні виклики сучасності та їх відображення в інформаційному просторі. *Правова інформатика*. 2012. № 2 (34). С. 19–27.
5. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>
6. Гурковський В. І. Безпека як об'єкт правовідносин в умовах глобального інформаційного суспільства: методологічний аспект. *Правова інформатика*. 2010. № 2(26). С. 72–77.
7. Мусієнко І. І. Інформаційно-психологічні аспекти безпеки суб'єктів сектору державної безпеки. *Правова інформатика*. 2012. № 4(36). С. 76–82.
8. Юдін О. К., Богуш В. М. Інформаційна безпека держави: навчальний посібник. Харків: Консум, 2005. с. 576.
9. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241

10. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України № 392/2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#Text>
11. Про основні засади забезпечення кібербезпеки України від 5 жовтня 2017 року № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403.
12. Косілова О. І. Інформаційна безпека України в умовах глобалізації. *Правова інформатика*. 2010. № 3 (27). С. 22–28.
13. Панченко О. А., Панченко Л. В. Інформаційна безпека та інформаційна культура в сучасному інформаційному суспільстві. *Правова інформатика*. 2015. № 2(46). С. 32–38.
14. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2021 року № 685/2021. URL: <https://www.president.gov.ua/documents/6852021-41069>
15. Марущак А. І. Дослідження проблем інформаційної безпеки у юридичній науці. *Правова інформатика*. 2010. № 3(27). С. 17–21.
16. Куренда Л. Д. Окремі аспекти забезпечення інформаційної безпеки Європейського Союзу. *Правова інформатика*. 2011. № 3–4(31). С. 36–42.