

Наумчук К.М.,
доцент кафедри національної безпеки,
публічного управління та адміністрування
Державний університет «Житомирська політехніка»
місто Житомир
Коршак В.С.,
Державний університет «Житомирська політехніка»
місто Житомир

ПРАВОВИЙ ЗАХИСТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВІЙНИ

Захист інформації є надзвичайно важливим етапом становлення національної безпеки кожної країни. Якщо враховувати те, що не лише повномасштабне вторгнення але й гібридна війна призводить до катастрофічних руйнацій, підриває довіру громадян до влади – виникає необхідність прийняття швидких рішень з боку держави, тому актуальність правового захисту інформаційної безпеки активізується як ніколи. Для усвідомлення усієї важливості нам необхідно розглянути, що ж являє собою інформація. Законодавче визначення поняття «інформація» міститься у Законі України «Про інформацію», згідно зі ст. 1 якого: «Інформацією є будь-які відомості та/або дані, що можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [7]. Аналогічне визначення міститься у ч. 1 ст. 200 Цивільного кодексу України [1]. Деталізоване визначення поняття «інформація» зазначене в іншому нормативно-правовому акті – Законі України «Про захист економічної конкуренції»: це відомості в будь-якій формі й вигляді та збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості; (ст. 1 Закону [6]).

Виходячи з вищезазначеного слід зауважити, що всі визначення поняття інформації є схожими, адже кожне стосується відображених відомостей які зберігаються у різній формі та є важливими для подальшого застосування. Тому, варто також розглянути поняття «інформаційна безпека». Згідно із Законом України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», інформаційна безпека - стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [11 р.ІІІ, п.10].

Оскільки інформаційна безпека є складним, системним, багаторівневим явищем, на стан і перспективи розвитку якого мають безпосередній вплив зовнішні та внутрішні чинники, розглянемо найважливіші з них, а саме:

- 1) політична обстановка у світі відноситься до зовнішніх чинників, наслідки яких не завжди можна спрогнозувати;
- 2) наявність потенційних зовнішніх і внутрішніх загроз;
- 3) стан і рівень інформаційно-комунікаційного розвитку країни є внутрішнім чинником, що свідчить про нашу конкурентоспроможність та готовність протистояти ворогові;
- 4) внутрішньополітична обстановка в державі.

Водночас інформаційна безпека є складною, динамічною, цілісною соціальною системою, компонентами якої є підсистеми безпеки особистості, держави і суспільства. Саме взаємозалежна, системна інформаційна єдність останніх складає якісну визначеність, покликану здійснити захист життєво важливих інтересів людини, суспільства і держави, забезпечити їх конкурентоздатний, прогресивний розвиток [15, с. 154–155]. Забезпечення інформаційної безпеки завдяки послідовній реалізації грамотно сформульованої національної інформаційної стратегії значною мірою може сприяти забезпеченню досягнення успіху при вирішенні завдань у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах державної діяльності. Так, втілення в життя вдалої інформаційної політики може суттєво вплинути на розв'язання внутрішньополітичних, зовнішньополітичних і військових конфліктів.

Специфіка забезпечення національної інформаційної безпеки відображена в Законах України «Про національну безпеку України» [10], «Про Концепцію Національної програми інформатизації» [9], «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [11], а також у затвердженій указом Президента Стратегії національної безпеки України [12], у зв'язку з реалізацією Стратегії Національна рада безпеки і оборони України ухвалила рішення про створення спеціального нового органу як робочого органу – Національного координаційного центру кібербезпеки. Створення такого центру є обґрунтованим, оскільки повноваженнями щодо забезпечення інформаційної безпеки наділена значна кількість державних органів та установ (Національна рада України з питань телебачення і радіомовлення, Держкомтелерадіо України, Служба безпеки України, Служба зовнішньої розвідки України, Міністерство оборони України, МВС України, Міністерство закордонних справ України, Міністерство юстиції України та ін.).

Значна кількість норм, що регулюють державний вплив в інформаційній сфері, вимагає їх певної класифікації для системного сприйняття. Найбільш доцільним для цілей нашого дослідження є їх розмежування за призначенням у системі державного управління, а також за об'єктом державного регулювання. Залежно від призначення тієї чи іншої правової норми в регулюванні функціонування складових елементів інформаційної сфери ці норми можливо об'єднати в такі чотири групи: 1) норми, що закріплюють цілі, основні завдання та напрями діяльності держави в інформаційній сфері, визначають основні параметри розвитку останньої. Ця група норм, до яких належать, зокрема, норми, закріплені у ст. 3, 10, 17, 31, 32, 34 Конституції, у ст. 6 Закону України «Про інформацію» [7], в розділах IV, VI Закону «Про Концепцію Національної програми інформатизації» [9], Законі «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [11] та в інших, має цілеспрямовуюче

значення для функціонування всієї системи державного управління в інформаційній сфері; 2) норми, що визначають систему органів (суб'єктів) державного регулювання в інформаційній сфері та їх адміністративно-правовий статус. До таких норм належать вже згадані норми Конституції України, які стосуються Держкомтелерадіо та Національної ради. Правовий статус окремих органів влади визначається і нормами законів. Так, у ст. 20 Закону «Про Кабінет Міністрів України» серед його повноважень згадується проведення державної політики у сфері інформатизації, сприяння становленню єдиного інформаційного простору та ін. [8]. Важливе місце в цій групі норм займають також норми, закріплені в підзаконних нормативно-правових актах, передусім ті з них, що містяться в актах Президента України та Кабінету Міністрів України, якими визначається адміністративно-правовий статус міністерств, інших органів державного управління в інформаційній сфері; 3) норми, що регулюють порядок взаємодії органів (суб'єктів) влади з керованими ними суб'єктами інформаційних та інформаційно-інфраструктурних відносин у процесі реалізації прямих і зворотних зв'язків між ними. До цієї групи належать норми, які регламентують процедури застосування різних методів державного регулювання в інформаційній сфері, визначають форми їх реалізації. Такі норми закріплені, зокрема, у ст. 23–37 Закону «Про телебачення і радіомовлення», які регламентують процедуру здійснення такого методу регулювання, як ліцензування в галузі телебачення і радіомовлення [13].

У Законі «Про друковані засоби масової інформації (пресу) в Україні» врегульовано порядок здійснення обов'язкової державної реєстрації друкованих засобів масової інформації [5]. У ст. 22 Закону «Про державну таємницю» регламентовано порядок надання допуску громадян до державної таємниці [3]. Застосування цілої низки заходів адміністративного примусу врегульовано нормами Кодексу України про адміністративні правопорушення [16]. У цих же законах та інших нормативно-правових актах визначаються і вимоги до форми правових актів, що приймаються при застосуванні зазначених методів. Після тривалих дискусій у 2011 р. законодавчу базу країни поповнив закон «Про доступ до публічної інформації» [4], яким встановлено більш ефективні механізми звернення до органів державної влади для отримання інформації, яка перебуває в їх розпорядженні; 4) норми, що визначають адміністративно-правовий статус суб'єктів інформаційних відносин. Так, наприклад, ст. 39 Закону «Про телекомунікації» на операторів телекомунікацій покладаються обов'язки: своєчасно надавати щорічно до центрального органу виконавчої влади в галузі зв'язку інформацію про свої телекомунікаційні мережі для відпрацювання мобілізаційних планів; за власні кошти встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів, і забезпечувати функціонування цих технічних засобів, а також сприяти проведенню оперативно-розшукових заходів тощо [14].

Стратегія національної безпеки України актуальними загрозами національній безпеці України в інформаційній сфері визначає ведення інформаційної війни проти України та відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства [2, с. 12]. Не менш гостро в умовах

гібридної війни постає питання кібербезпеки. У сучасному світі кібернетичний простір дедалі частіше слугує для проведення широкого спектра підривних операцій: від викрадення цінної інформації до актів кібертероризму [17, с. 18].

Загалом політика інформаційної безпеки як суспільне явище має комплексний характер, включаючи внутрішньо та зовнішньополітичні, економічні, технологічні, військові та інші елементи, тому вимагає комплексного підходу. Діяльність органів державної влади повинна спрямовуватися на виконання конкретних завдань у цій сфері й об'єднуватися єдиною метою – надання належних умов для реалізації забезпечення інформаційної безпеки України. Система інформаційної безпеки держави є складовою частиною загальної системи національної безпеки країни та становить сукупність органів державної влади, недержавних структур і громадян, які повинні узгоджено здійснювати діяльність по забезпеченню інформаційної безпеки на основі єдиних правових норм, ефективно протистояти інформаційним загрозам за сучасних умов.

Список використаних джерел:

1. Цивільний кодекс України URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>
2. Бєлай С.В., Корнієнко Д.М. Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки. Актуальні проблеми управління інформаційною безпекою держави. Київ : Національна академія Служби безпеки України, 2018. 408 с.
3. Закон України «Про державну таємницю» URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text>
4. Закон України «Про доступ до публічної інформації» URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
5. Закон України «Про друковані засоби масової інформації (преси) в Україні» URL: <https://zakon.rada.gov.ua/laws/show/2782-12#Text>
6. Закон України «Про захист економічної конкуренції» URL: <https://zakon.rada.gov.ua/laws/show/2210-14#Text>
7. Закон України «Про інформацію» URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
8. Закон України «Про Кабінет міністрів України» URL: <https://zakon.rada.gov.ua/laws/show/794-18#Text>
9. Закон України «Про Концепцію Національної програми інформатизації» URL: <https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text>
10. Закон України «Про національну безпеку України» URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
11. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» URL: <https://zakon.rada.gov.ua/laws/show/537-16#Text>
12. Указ Президента України «Про Стратегію національної безпеки України» URL: <https://www.president.gov.ua/documents/3922020-35037>
13. Закон України «Про телебачення і радіомовлення» URL: <https://zakon.rada.gov.ua/laws/show/3759-12#Text>

14. Закону України «Про телекомунікації» URL:
<https://zakon.rada.gov.ua/laws/show/1280-IV#Text>
15. Золотар О.О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.
16. Кодекс України про адміністративні правопорушення URL:
<https://zakon.rada.gov.ua/laws/show/80731-10#Text>
17. Гуржій Т. Інформаційне право: виклики гібридної війни. Зовнішня торгівля: економіка, фінанси, право. 2018. № 4. С. 16–26.