УДК 36.7:340.5:347.7(045)
DOI https://doi.org/10.32782/2524-0374/2023-4/3

ПЕРСПЕКТИВИ РОЗВИТКУ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ВІЙНІ

PROSPECTS FOR THE DEVELOPMENT OF LEGAL SECURITY AGAINST INFORMATION WARFARE

Басенко Р.О., к.п.н., доцент,
завідувач кафедри правознавства та фінансів, заступник директора з науково-педагогічної роботи, міжнародної та грантової діяльності
Полтавський інститут економіки і права Закладу вищої освіти «Відкритий міжнародний університет розвитку людини «Україна»

Шаравара Р.І., к.е.н., доцент,
професор кафедри правознавства та фінансів, перший заступник директора
Полтавський інститут економіки і права Закладу вищої освіти «Відкритий міжнародний університет розвитку людини «Україна»

Кравченко А.П., к.ю.н., доцент,
доцент кафедри правознавства та фінансів
Полтавський інститут економіки і права Закладу вищої освіти «Відкритий міжнародний університет розвитку людини «Україна»

Чумаш Д.О., здобувачка вищої освіти зі спеціальності 081 Право
Полтавський інститут економіки і права Закладу вищої освіти «Відкритий міжнародний університет розвитку людини «Україна»

У центрі уваги авторів статті – обґрунтування перспектив розвитку нормативно-правового забезпечення протидії сучасній інформаційній війні. Зокрема розглянуто основні виклики, які ставить перед сучасною безпекою суспільства інформаційна війна; визначено та обґрунтовано необхідність заходів щодо удосконалення правового забезпечення протидії інформаційній агресії; окреслено перспективи розвитку сучасного інформаційного права у контексті застосування агресором дезінформаційних методів боротьби.

Доведено, що протидія інформаційній агресії потребує відповідного законодавчого та нормативно-правового забезпечення, у тому числі формування та реалізації правових норм, а також правотворчої та правозастосовчої діяльності. Виявлено, що правотворча діяльність щодо формування інформаційної політики у сфері інформаційної безпеки тісно пов'язана з формуванням якісного інформаційного законодавства. Виокремлено два виміри нормативно-правового забезпечення протидії інформаційній війні 1) правова база в інформаційній сфері; 2) правозастосовча практика в інформаційній сфері. Констатовано, що правова організація діяльності щодо забезпечення інформаційної безпеки держави означає впорядкування, узгодження взаємопов'язаних систем та норм інформаційної діяльності, положень інформаційного права, необхідних для набуття створення умов для інформаційної безпеки.

Виокремлено складники стратегії боротьби з дезінформацією та пропагандою: створення законодавчої бази для моніторингу та контент-аналізу інформаційного простору, ведення необхідного контролю щодо медіа та соціальних мереж з метою виявлення дезінформації та пропаганди; розробки та впровадження системи швидкого реагування на дезінформацію, як-от внесення змін до законодавства щодо формування команд швидкого реагування на поширення дезінформації та пропаганди; забезпечення доступної та достовірної інформації для громадськості щодо реальних подій з механізмами виключення можливості маніпулювання нею; розвитку системи тренінгів та інших інформаційних проєктів щодо медійної грамотності серед громадян та посилення навичок критичного мислення; укладення необхідної міжнародної правової основи для ефективної співпраці з зарубіжними партнерами та використання їхнього досвіду боротьби з дезінформацією та пропагандою, забезпечення безпеки інформаційного простору тощо.

Зроблено висновок про необхідність удосконалення нормативно-правової бази щодо формування цілісної стратегії протидії інформаційній війні, яка базувалася б на прозорості, правдивій інформації, підвищенні медійної грамотності громадян.

Ключові слова: інформаційна війна, нормативно-правове забезпечення, інформаційне право, інформаційна політика, інформаційне законодавство, інформаційна безпека, гібридна агресія.

The focus of the authors of the article is the substantiation of the prospects for the development of legal support for countering the modern information war. In particular, the main challenges that the information war poses to the modern security of society are considered; identified and substantiated the need for measures to improve the legal support for combating information aggression; the prospects for the development of modern information law in the context of the use of disinformation methods of struggle by the aggressor are outlined.

It has been proved that counteracting information aggression requires appropriate legislative and regulatory support, including the formation and implementation of legal norms, as well as law-making and law enforcement activities. It has been established that law-making activity on the formation of information policy in the field of information security is closely related to the formation of high-quality information legislation. Two dimensions of the legal framework for counteracting information warfare are identified: 1) the legal framework in the information sphere; 2) law enforcement practice in the information sphere. It is stated that the legal organization of activities to ensure the information security of the state means streamlining, harmonizing interconnected systems and norms of information activity, the provisions of information law necessary to create conditions for information security.

The components of the strategy to combat disinformation and propaganda are identified: the creation of a legislative framework for monitoring and content analysis of the information space, maintaining the necessary control of the media and social networks in order to identify disinformation and propaganda; developing and implementing a rapid response system to disinformation, such as amending the legislation to form rapid response teams to disseminate disinformation and propaganda; providing accessible and reliable information for the public about real events with mechanisms to exclude the possibility of manipulating it; developing a system of trainings and other information projects on media literacy among citizens and strengthening critical thinking skills; conclusion of the necessary international legal framework for effective cooperation with foreign partners and the use of their experience in combating disinformation and propaganda, ensuring the security of the information space, etc.

It is concluded that it is necessary to improve the regulatory framework for the formation of a holistic strategy to counter the information war, which would be based on transparency, truthful information, and increasing the media literacy of citizens.

Key words: information war, legal support, information law, information policy, information legislation, information security, hybrid aggression.

Ключове значення у сучасному постіндустріальному та інноваційному суспільстві відіграє інформація. Діалектичний статус інформації виявляється у її здатності відігравати роль основного блага і водночас бути інструментом ведення війн та насильства. У цьому контексті варто розглядати сутність нинішнього гібридного протистояння в світі, яке має відбиток й в Україні. На тлі повномасштабної війни в Україні з'явилася нова загроза – інформаційна війна, яка стала одним з найефективніших засобів ведення боротьби проти суверенності та соборності держави. Агресія щодо суверенітету України виявилася не лише у військовому вторгненні, але й стала атакою на інформаційну сферу країни, що становить серйозну загрозу національній безпеці. Це є серйозним викликом для правової сфери та суспільної свідомості, оскільки інформаційна війна дає можливість маніпулювати громадською думкою, здатна спричинити дестабілізацію внутрішньої ситуації та поширення інформаційних фейків. У зв'язку з цим, проблематика розвитку правового забезпечення протидії інформаційній війні в Україні стає особливо актуальною і потребує ефективної стратегії та відповідного законодавчого забезпечення.

Із огляду на високий ступінь актуальності, аналіз шляхів удосконалення нормативно-правового регулювання інформаційної безпеки був предметом багатьох досліджень. Зокрема слід окремо відзначити наукові доробки таких дослідників, як В. Гурковський, Ю. Коваленко, І. Корж, Л. Кочубей, Д. Кунєв, Ю. Максименко, О. Олійник, В. Остроухов, Є. Рогова, В. Ярочкін та інші. Водночас, динамічність розвитку технологій, методів та прийомів ведення інформаційної війни потребує нових підходів до запобігання та протидії такій гібридній агресії, а відтак й оновлення правового забезпечення такої безпекової діяльності.

Мета дослідження – обґрунтувати перспективи розвитку нормативно-правового забезпечення протидії інформаційній війні. Зокрема необхідно розглянути основні виклики, які ставить перед сучасною безпекою суспільства інформаційна війна; визначити та обґрунтувати необхідність заходів щодо удосконалення правового забезпечення протидії інформаційній агресії; окреслити перспективи розвитку сучасного інформаційного права у контексті застосування агресором дезінформаційних методів боротьби.

Не потребує доведення теза про те, що інформаційна війна є серйозним викликом для світу загалом і для України зокрема, оскільки її мета полягає у руйнуванні сутнісного бачення світу, деформації демократичних інститутів, посиленні деструктивного впливу на національну свідомість та збуренні суспільства.

З-поміж основних викликів, які ставить інформаційна війна виокремлюють: дезінформацію та фейкові новини, що викликають паніку та невизначеність у населення; маніпуляції національною свідомістю, які можуть спричинити ворожнечу до інших країн, релігійних та етнічних груп, відчуття агресії до власної держави; кібератаки на державні інформаційні системи, що може призвести до порушення роботи урядових установ, банків, медичних закладів та інших важливих інфраструктурних об'єктів; використання соціальних мереж та медіа-платформ для дезінформації та маніпулювання національною свідомістю.

Методи, що використовуються в інформаційній війні, включають в себе підривну пропаганду, дезінформацію, психологічні операції, кібератаки та інші засоби, які допомагають досягти мети інформаційної війни – знищення державного суверенітету та здобуття контролю над державою. Для протидії інформаційній війні, Україна вживає різноманітні комплексні заходи, такі як підвищення інформаційної грамотності населення, розвиток сучасних інформаційних технологій, створення необхідних інструментів для ефективної діяльності систем кібербезпеки тощо [4, с. 93].

Нині Україна веде активну боротьбу з інформаційною війною. Сьогодні є необхідне правове поле для успішної протидії інформаційній агресії, зокрема: діє Національна рада з питань телебачення і радіомовлення, яка відповідає за регулювання медіа в Україні і забезпечення дотримання законодавства про медіа; удосконалюється Закон України «Про інформацію», який регулює питання збору, обробки, зберігання, захисту та поширення інформації в Україні; створюються центри кібербезпеки, які забезпечують захист від кібератак, здійснюють виявлення та протидію загрозам в інформаційному просторі; значна увага приділяється розвиткові медійної грамотності серед громадян, освіти у галузі кібербезпеки, навчанню щодо виявлення та запобігання дезінформації [1, с. 105]; динамічно зростає рівень співпраці з міжнародними партнерами, зокрема з Європейським Союзом та НАТО, для спільної боротьби з інформаційною агресією. Однак, не зважаючи на застосовані заходи, Україна продовжує зіштовхуватися з викликами інформаційної війни, які вимагають подальшого вдосконалення нормативно-правової бази загальної стратегії протидії інформаційній агресії [7, с. 157].

Проблема підвищення інформаційної безпеки загострюється під час зовнішніх загроз, зокрема інформаційної війни. У таких умовах звичайні засоби та методи інформаційної діяльності використовуються як стандартні, але значно зростає необхідність їхнього прогнозування, що вимагає відповідного правового регулювання. Протидія інформаційної агресії потребує відповідного законодавчого та нормативно-правового забезпечення, у тому числі формування та реалізації правових норм, а також правотворчої та правозастосовчої діяльності. Правотворча діяльність щодо формування інформаційної політики у сфері інформаційної безпеки тісно пов'язана з формуванням якісного інформаційного законодавства на основі уявлення про стан його: 1) правової бази в інформаційній сфері; 2) правозастосовчої практики в інформаційній сфері. Ми згодні з думкою Д. Кунєва про те, що правова організація діяльності щодо забезпечення інформаційної безпеки держави означає впорядкування, узгодження взаємопов'язаних систем норм інформаційної діяльності та норм інформаційного права, необхідних для набуття якостей та закріплення закономірностей, що забезпечують ефективність та розвиток певних видів діяльності та відповідної соціальної системи [3, с. 95, 100].

Із точки зору змісту інформаційної безпеки цінним уважаємо виділення В. Роговою двох найважливіших видів інформаційної безпеки: 1) інформаційна безпека особистості, як захист психіки та свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформація, підбурювання до правопорушень, суїциду тощо. Застосування таких технологій може призвести до значних структурно-функціональних змін свідомості та психічної діяльності людини; 2) інформаційна безпека держави – ступінь захищеності держави (суспільства) та стійкості основних сфер її життя (економіки, науки, техносфери, управління, військової справи тощо) від дестабілізуючих інформаційних впливів. Інформаційна безпека визначається можливістю нейтралізації таких дій [6, с. 193].

Крім того, В. Рогова зазначала, що до суттєвих ознак інформаційної безпеки відносяться конфіденційність (стан інформації, при якому доступ до неї отримують лише суб'єкти, які мають на це право), цілісність (запобігання несанкціонованій або неправомірній зміні інформації) та доступність (запобігання) тимчасове або постійне приховування інформації від користувачів, які отримали право доступу), відмовостійкість (здатність засвідчити дію або подію, що відбулася, щоб ці події згодом не могли бути відкинуті), підзвітність, достовірність, автентичність [6, с. 195].

На нашу думку, ефективна стратегія боротьби з дезінформацією та пропагандою, насамперед, потребує відповідного нормативно-правове забезпечення щодо здійснення таких заходів:

1) створення законодавчої бази для моніторингу та контент-аналізу інформаційного простору, ведення необхідного контролю щодо медіа та соціальних мереж з метою виявлення дезінформації та пропаганди;

2) розробки та впровадження системи швидкого реагування на дезінформацію, як-от внесення змін до законодавства щодо формування команд швидкого реагування на поширення дезінформації та пропаганди;

3) забезпечення доступної та достовірної інформації для громадськості щодо реальних подій з механізмами виключення можливості маніпулювання нею;

4) розвитку системи тренінгів та інших інформаційних проєктів щодо медійної грамотності серед громадян та посилення навичок критичного мислення;

5) укладення необхідної міжнародної правової основи для ефективної співпраці з зарубіжними партнерами та використання їхнього досвіду боротьби з дезінформацією та пропагандою, забезпечення безпеки інформаційного простору;

6) розвитку інноваційних технологій для виявлення та протидії дезінформації та пропаганди, використання новітніх систем, як-от штучний інтелект та блокчей тощо [2, с. 99].

Цінна з погляду впорядкування правового забезпечення інформаційної безпеки є запропонована О. Олійником структура нормативно-правових актів, зокрема виокремлюються такі правові блоки: 1) конституційне законодавство, що акумулює норми з питань інформатизації, інформаційної безпеки тощо; 2) загальні закони, кодекси (про власність, про надра, про землю, про права громадян, про громадянство, про податки, про антимонопольну діяльність тощо), що включають норми з питань захисту інформації; 3) закони про організацію управління, що стосуються окремих структур господарства, економіки, системи державних органів та визначають їх статус (включають окремі норми забезпечення інформаційної безпеки, поряд із загальними питаннями інформаційного забезпечення та інформаційної безпеки конкретного органу, ці норми повинні встановлювати його обов'язки щодо формування, актуалізації інформаційної безпеки, що становить загальнодержавний інтерес; 4) спеціальні закони, що регулюють окремі сфери відносин, галузі економіки, процеси (Закон України «Про інформацію» та інші, зміст яких створює спеціальне законодавство як основу правового забезпечення інформаційної безпеки); 5) підзаконні акти щодо забезпечення інформаційної безпеки; 6) законодавство України, яке містить норми про відповідальність за правопорушення у сфері захисту інформації [5, с. 135]. Уважаємо, що саме така структура відіграє роль методологічних орієнтирів для удосконалення відповідних норм інформаційного права.

Висновки. Сучасні умови, в яких опинилася Україна свідчать, війна не обмежується лише бойовими діями та включає у себе велику кількість інформаційних аспектів, в тому числі дезінформацію, пропаганду, кібератаки та інші методи, що допомагають ворогу займати позиції в медіапросторі та впливати на свідомість населення. Інформаційна війна є складною і довготривалою боротьбою, яка вимагає постійного оновлення стратегій та тактик протидії. Перевага сторін може залежати від багатьох чинників, включаючи правову, політичну, економічну та військову ситуацію в регіоні, рівень та ефективність захисту інформаційного простору України. Успішною стратегією для України є збереження незалежного та вільного інформаційного простору, де громадяни мають доступ до різноманітної та правдивої інформації, здійснення ретельного контролю над поширенням дезінформації та пропаганди. Для цього необхідно удосконалювати інформаційне законодавство, яке б забезпечило появу інноваційних технологій боротьби з інформаційною війною, створило б необхідне правове підгрунтя для підвищення медіа грамотності серед населення та активного залучення міжнародної спільноти до протидії інформаційній війні.

Сьогодні гостро постає необхідність удосконалення нормативно-правової бази щодо формування цілісної стратегії протидії інформаційній війні, яка базувалася б на прозорості, правдивій інформації, підвищенні медійної грамотності громадян. Важливим елементом в такій стратегії є активна робота з медіа та громадськістю, підтримка незалежних ЗМІ та обмеження впливу інформаційних ресурсів, що діють на користь ворога. Виняткову важливість становить формування законодавчих підстав для активізації освітньої та культурно-просвітницької діяльності щодо збільшення рівня свідомості населення шляхом інформування його про ситуацію в країні із достовірних джерел інформації. Це надасть змогу людям бути більш обізнаними та здатними до самостійного аналізу та оцінки інформації, що вони отримують. Крім того, нагальною є потреба проведення відповідних законодавчих змін щодо вироблення технологій запобігання можливому втручанню ворога в електронні системи установ та підприємств критичної інфраструктури.

ЛІТЕРАТУРА

1. Бакалінська О., Бакалінський О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право.* 2019. № 9. С. 100–108.

2. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навчальний посібник. Київ : Кондор, 2008. 384 с.

3. Кунєв Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження. *Юридичний вісник.* 2021. № 1. С. 95–102.

4. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки. *Державна безпека України.* 2011. № 21. С. 92–95.

5. Олійник О. Нормативно-правове забезпечення інформаційної безпеки в Україні. *Право і суспільство*. 2012. № 3. С. 132–137.

6. Рогова Є. І. Теоретичні основи правового забезпечення інформаційної безпеки. *Актуальні проблеми держави і права* : зб. наук. пр. / редкол.: Г. І. Чанишева (голов. ред.) та ін. Одеса : Гельветика, 2020. Вип. 86. С. 190–196.

7. Северина С. В. Інформаційна безпека та методи захисту інформації. *Вісник Запорізького національного університету.* 2016. № 1 (29). С. 155–161.