

УДК 342.9:004.056.53:327.8(470:477)

DOI <https://doi.org/10.24144/2307-3322.2025.90.3.57>

УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАКОНОДАВСТВА ЯК НАПРЯМ ПРОТИДІЇ РОСІЙСЬКІЙ ІНФОРМАЦІЙНІЙ АГРЕСІЇ

Солодка О.М.,
*кандидат юридичних наук,
старший науковий співробітник,
Національна академія СБ України
ORCID: 0000-0002-1799-0712*

Солодка О.М. Удосконалення інформаційного законодавства як напрям протидії російській інформаційній агресії.

Результати дослідження вказують на те, що удосконалення вітчизняного інформаційного законодавства є важливим елементом протидії російській інформаційній агресії і загалом можна виокремити дві складові цієї діяльності: перша – це розвиток вітчизняної інформаційної сфери з метою забезпечення участі України як повноправного учасника міжнародного інформаційного обміну, долучення її до європейських ініціатив, друга – це вироблення механізмів протидії проявам інформаційної агресії РФ – дезінформації, пропаганді, ІПСО, FIMI тощо.

Пріоритетним напрямками визначено: вироблення дієвих правових механізмів захисту інформаційного суверенітету України, які б забезпечили розвиток українського суспільства в дусі національної гідності, патріотизму та національної свідомості з дотриманням принципів захисту прав, свобод і безпеки людини та законних інтересів суспільства і держави в інформаційній сфері; упорядкування інформаційної діяльності в національному вимірі з метою її ефективної координації на державному рівні, формування національної системи забезпечення інформаційної безпеки, в тому числі побудови ефективної системи стратегічних комунікацій як скоординованої взаємодії органів державної влади з громадянським суспільством; удосконалення комплексу заходів із протидії негативним інформаційним впливам, посилення спроможностей сектору безпеки і оборони щодо протидії спеціальним інформаційним операціям, спрямованим на зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності, підірив обороноздатності України, деморалізацію особового складу Збройних сил України та інших військових формувань, загострення суспільно-політичної ситуації, поширення інформації з обмеженим доступом; посилення юридичної відповідальності суб'єктів українського інформаційного простору, що створені та/або використовуються державою-агресором для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності, зокрема встановлення юридичної відповідальності за умисне систематичне поширення неправдивої інформації, яка створює загрозу суверенітету, територіальній цілісності та недоторканості України, обороноздатності, інформаційній безпеці держави, особливо під час дії правового режиму воєнного стану.

Ключові слова: інформаційне законодавство, інформаційна безпека та суверенітет, інформаційна агресія, протидія інформаційній агресії.

Solodka O.M. Improving information legislation as a way to counter russian information aggression.

The results of the study indicate that improving domestic information legislation is an important element of countering russian information aggression and in general, two components of this activity can be distinguished: the first is the development of the domestic information sphere in order to ensure Ukraine's participation as a participant in international information exchange, including it in European initiatives, the second is to develop mechanisms to counter the manifestations of information aggression of the russian federation – disinformation, propaganda, IPSO, FIMI, etc.

The priority areas are: developing effective legal mechanisms to protect Ukraine's information sovereignty, which would ensure the development of Ukrainian society in the spirit of national dignity,

patriotism and national consciousness, while adhering to the principles of protecting human rights, freedoms and security and the legitimate interests of society and the state in the information sphere; streamlining information activities at the national level with the aim of its effective coordination at the state level, forming a national information security system, including building an effective system of strategic communications as a coordinated interaction between state authorities and civil society; improving the set of measures to counter negative information influences, strengthening the capabilities of the security and defense sector to counter special information operations aimed at changing the constitutional order by force, violating sovereignty and territorial integrity, and undermining Ukraine's defense capabilities, demoralization of the personnel of the Armed Forces of Ukraine and other military formations, aggravation of the socio-political situation, dissemination of information with limited access; strengthening the legal responsibility of subjects of the Ukrainian information space, which are created and/or used by the aggressor state to wage information war against Ukraine and preventing their subversive activities, in particular establishing legal liability for the deliberate systematic dissemination of false information that poses a threat to the sovereignty, territorial integrity and inviolability of Ukraine, defense capability, information security of the state, especially during the legal regime of martial law.

Key words: information legislation, information security and sovereignty, information aggression, counteraction to information aggression.

Постановка проблеми. Посилення інформаційних атак і операцій рф щодо України в умовах стрімкого розвитку інформаційних технологій та зростання залежності сучасного суспільства від інформації робить реалізацію національних інтересів України в інформаційній сфері важливим чинником національної безпеки та обумовлює необхідність розроблення цілісної гнучкої державної політики у сфері забезпечення інформаційної безпеки, яка враховуватиме багатоаспектність цього явища, агресію рф, перспективні тенденції змін інформаційного простору, особливості геополітичного становища і знайде своє відображення на правовому рівні в ефективному інформаційному законодавстві, адже незадовільність рівня останнього та необхідність вжиття заходів щодо його удосконалення є очевидними. За умови подальшого збереження належної правової урегульованості інформаційних відносин фактично створюються всі передумови для розвитку інформаційного контролю, який пронизує усі сфери. Разом з тим, можемо констатувати відсутність консенсусу у шляхах належної трансформації інформаційного законодавства України серед дослідників цієї проблематики, зважаючи на складність, динаміку та масштабність сучасних інформаційних процесів, умови воєнного стану, диверсифікацію інформаційних технологій тощо, що обумовлює актуальність дослідження.

Аналіз останніх досліджень і публікацій. У сучасній науковій літературі питання протидії інформаційній агресії рф та удосконалення інформаційного законодавства знайшли відображення у численних наукових працях, зокрема Пилипчук В.Г., Довгань О.Д., Красноступ Г.М., Корж І.Ф., Панченко В.М., Тихомиров О.О. та багато інших, проте розвиток інформаційного суспільства.

Метою статті є визначення напрямів удосконалення інформаційного законодавства як напрямом протидії російській інформаційній агресії.

Виклад основного матеріалу. Ступінь інтеграції будь-якої держави в інформаційне суспільство визначається наявністю концепції державної інформаційної політики, правовим забезпеченням інформаційного суспільства, розвитком інформаційної та комунікаційної інфраструктури, багатством інформаційних ресурсів, динамікою інформаційного ринку, міжнародним співробітництвом у галузі інформації. Сьогодні розвиток інформаційних процесів має глобальний характер, а в міжнародних програмах декларуються приблизно однакові положення, проте кожна країна світу визначає власний шлях. Хоча в Україні лише триває процес формування та становлення інформаційного суспільства, але вона демонструє послідовне і стійке просування до поставленої мети, адже поступово формується відповідна законодавча база, впроваджуються новітні технології, створюються і використовуються унікальні інформаційні ресурси, відбувається формування інформаційної культури. Проте, агресія проти нашої держави і прояви сепаратизму в окремих її регіонах зумовили перевірку системи національної безпеки на міцність. Така ситуація зумовила, з одного боку, необхідність вжиття рішучих заходів щодо відсічі агресії, з другого – продемонструвала неготовність вітчизняної правової системи до дії в екстремальних умовах. Численні недоліки законодавства зумовили екстраординарний характер реагування, що призвело до виникнення ускладнених законодавчих конструкцій, частина з яких, з огляду на низку причин, відразу вияви-

ла власну нежиттєздатність, інші натомість значно ускладнили стан правового регулювання суспільних відносин [1, с. 26]. Разом з тим, не набули подальшого впровадження правові положення щодо законодавчого врегулювання питань розвитку національного інформаційного простору.

Сучасні українські дослідники виокремлюють означальні риси інформаційної агресії, яка є релевантною теперішній українській ситуації, а саме: несиловий характер, відсутність підпорядкування фізичним закономірностям (немає маси, ваги, розміру, температури тощо); нелінійність, тобто непропорційна залежність причини й наслідку, порушення закону збереження матерії та енергії, кумулятивний характер, можливість лавиноподібного зростання інформації; можливість максимальної дальності й швидкості розповсюдження, що зростає з розвитком інформаційних технологій; можливість ідеального клонування; нелокалізованість у часі – наслідки інформаційної агресії і насилля можуть бути розмитими у часі й просторі; пандемічність, опосередкований характер і потаємність впливу (інформаційна дія має глобальний характер й на відміну від фізичного впливу може бути абсолютно непомітною); віртуальний характер дії, можливість фокусування, селективність, уразливість (крихкість інформаційного світу, легкість доступу, можливість зламу інформаційних систем) [2].

При цьому потрібно враховувати необхідність збереження балансу між інтересами держави у сфері інформаційної безпеки та інформаційними правами людини, оскільки двома ключовими характеристиками сучасного історичного періоду є глобалізація та розвиток інформаційно-комунікаційних технологій, які виступають головною рушійною силою глобалізованих суспільств, в основі яких лежать знання та інформація, що призвело до формування нового типу суспільного устрою – інформаційного суспільства, яке існує і розвивається на двох рівнях – національному та міжнародному.

Мета правового регулювання, поставлена відповідно до принципів розвитку інформаційного суспільства, для досягнення необхідного результату вимагає органічного поєднання публічно-правових та приватно-правових засобів в структурі механізму правового регулювання. Це дозволить врахувати особливий характер інформаційної діяльності та інформаційного суверенітету. На думку І.Ф. Коржа, міцність правопорядку, авторитетність права значною мірою залежать від спроможності законодавця своєчасно враховувати відносини, що виникають і породжують спори, конфлікти, які потребують юридичного регулювання і захисту і які, насамперед, знаходять відображення в правозастосовній (судовій та адміністративній) практиці. Саме стабільна, авторитетна, динамічна правова система, яка забезпечена відповідним їй апаратом судової влади та правоохоронних органів – є найбільш ефективною формою упорядкування і динаміки суспільних відносин [3, с. 25].

Окрім цього, проголошення й конституційне закріплення стратегічного курсу держави на європейську та євроатлантичну інтеграцію зумовили необхідність адаптації вітчизняного законодавства до правових систем і стандартів у сфері безпеки та оборони країн-членів ЄС і НАТО. Проведення реформ, спрямованих на інтеграцію до глобального інформаційного простору, є одним із ключових зобов'язань України перед ЄС у межах виконання Угоди про асоціацію між Україною та Європейським Союзом [4], ратифікованої у вересні 2014 р. Зокрема, цим питанням присвячена Глава 14 Угоди (ст. 389-395), де зазначається, що сторони зміцнюють своє співробітництво з розвитку інформаційного суспільства на користь приватних осіб і бізнесу через забезпечення загальнодоступності ІКТ та через кращу якість послуг за доступними цінами, що, в свою чергу, полегшить доступ до ринків послуг електронних комунікацій і сприятиме конкуренції й надходженню інвестицій у цю галузь. Співробітництво має на меті імплементацію національних стратегій інформаційного суспільства, розвиток всеохоплюючої нормативно-правової бази для електронних комунікацій та розширення участі України в дослідницькій діяльності ЄС у сфері ІКТ. Сторони сприяють поступовому наближенню до права і нормативно-правової бази ЄС у галузі регулювання інформаційного суспільства й електронних комунікацій.

Динамічне формування глобального інформаційного простору, постійне зростання свободи комунікаційних і комп'ютерних мереж, швидкий розвиток інформаційних технологій, продуктів і послуг створюють принципово нові можливості для економічної співпраці, обміну інформацією, технологіями, духовними цінностями, взаємного культурного збагачення. Водночас проблеми інтеграції України в європейський інформаційний простір, які зумовлені дією внутрішніх і зовнішніх чинників, мають комплексний характер – охоплюють усі сфери життєдіяльності людини, суспільства та держави. Це, зокрема, неузгодженість термінології, основних положень та прин-

ципів вітчизняного законодавства з європейським, невідповідність стандартам розвинених країн окремих секторів інформаційного простору України. Крім того, слід звернути увагу й на такі проблемні моменти, як правова неврегульованість суспільних відносин, пов'язаних із формуванням, розвитком, використанням і захистом інформації, інформаційних прав, інформаційних ресурсів, інформаційної інфраструктури; відсутність єдиного узгодженого понятійно-термінологічного апарату інформаційної та кібербезпеки України тощо

В контексті останнього, слід підкреслити, що на сьогодні, незважаючи на значну вживаність аббревіатури FIMI (Foreign Information Manipulation and Interference) – «зовнішнє інформаційне маніпулювання та втручання» [5], яку у 2021 р. Робоча група зі стратегічних комунікацій та Відділ інформаційного аналізу ЄС у Звіті про свою роботу ввели як модель поведінки, яка загрожує або може негативно вплинути на цінності, процедури та політичні процеси; діяльність носить маніпулятивний характер, здійснюється цілеспрямовано та скоординовано; суб'єктами такої діяльності можуть бути державні чи недержавні суб'єкти, у тому числі їхні довірені особи на власній території та за її межами. У звіті визнають, що FIMI регулярно використовують для підриву довіри суспільства до легітимності та ефективності демократичних інститутів; воно може сприяти посиленню поляризації всередині ЄС й посилити ескалацію політичного насильства в уже схильних до конфліктів регіонах.

Наразі немає консенсусу щодо того, чим саме є «втручання», й чітко не розмежовано концепт «втручання» від інших суміжних понять та не визначено його співвідношення з поняттям інформаційної агресії, що може не лише затримати або ускладнити ініціативи законодавців, а й негативно позначитися на зусиллях громадянського суспільства щодо підвищення обізнаності суспільства та його згуртування у протидії втручанням у демократичні процеси. Проте експерти застерігають, що визначення втручання пов'язане з ризиком щодо визначення, яке є або занадто загальним, і відтак може створювати перешкоди свободі слова або навпаки, – занадто вузьким, щоб охопити усі форми протиправної поведінки у сферах, що наразі швидко розвиваються, й відтак це заважатиме ідентифікувати таку діяльність, а відтак і запровадити релевантні санкції та адекватні заходи протидії.

Російське інформаційне маніпулювання та втручання характеризується безпрецедентним масштабом, інтенсивністю та використанням широкого спектру інструментів – від державних медіа до приватних ботоферм, від кібератак до прямої пропаганди на окупованих територіях. Це не просто «один з» іноземних впливів, а скоординована стратегія, спрямована на дестабілізацію та знищення держав [5].

З огляду на глобальний характер загроз, пов'язаних із FIMI, ефективна протидія потребує єдиного та колективного підходу. Вкрай важливим є створення спільної системи класифікації та, за можливості, визначення джерел такої діяльності.

Дедалі більшої актуальності набуває інформаційно-гуманітарна безпека як держави і суспільства, адже загрози інформаційній безпеці набули екзистенційного характеру, спрямовані на знищення української державності, української національної та громадянської ідентичності та єдності. Це, в свою чергу, зумовлює необхідність створення й організації єдиної державної системи протидії негативним інформаційним впливам, куди б, окрім відповідних підрозділів уповноважених структур, активно залучалися для і цивільні аналітичні центри, PR-компанії та медіа на зразок взаємодії у кіберпросторі.

Крім того, організаційна структура органів державної влади, що формують та реалізують державну інформаційну політику в Україні, потребує реформування на основі науково обґрунтованих рішень, які засновані на глибокому аналізі чинних міжнародно-правових актів з питань інформатизації суспільства та національного законодавства різних країн у сфері створення інформаційного суспільства, протидії сучасним загрозам інформаційного характеру, зокрема в частині створення загальнонаціонального координаційного центру, який був би спроможним узгоджувати і координувати діяльність зазначених правоохоронних органів, силових структур і відомств щодо протидії реальним загрозам інформаційному і кіберпростору України;

Зазначимо, РФ значно посилсила інформаційні маніпуляції та втручання, у тому числі шляхом поширення дезінформації та пропаганди, реалізації спрямованих на деморалізацію українців інформаційних кампаній, підрив довіри до влади, поширення паніки, а також дискредитацію України на міжнародній арені. Обсяги та складність цих операцій багаторазово зросли, оскільки платформи як Telegram, WhatsApp, інші приватні месенджери стали ключовими каналами для

поширення дезінформації, що вимагає нових підходів до регулювання та співпраці з зазначеними суб'єктами. З цим питанням тісно пов'язана й проблема цифрових прав людини, особливо в контексті курсу країни на масштабну діджиталізацію.

Сучасний європейський дискурс зосереджений над вдосконаленням нормативної бази, пов'язаної з блокуванням поширення протиправного інформаційного контенту, протидії протиправному використанню ШІ технологій у тісній співпраці з офіційними представництвами інтернет-гігантів. В той же час, в Україні відсутні норми законодавства, які б регулювали діяльність ІТ-платформ та встановлювали чіткі правила роботи в цифровому просторі України, не визначенні повноваження органів державної влади України у цій сфері та порядок взаємодії, відсутні алгоритми реагування на інциденти, оскільки платформи мають свої встановлені правила, на порушення яких реагують.

Водночас у процесі розвитку перебуває урегулювання порядку функціонування в Україні суб'єктів медіа, поки не напрацьовано дієвої нормативно-правової бази, яка б дозволяла обмежувати негативний вплив соціальних мереж на суспільство. Відсутні перепони для поширення серед інтернет-користувачів інформації та рекомендацій, що розпалюють расову і релігійну нетерпимість, деструктивні й агресивні настрої і згубно впливають на психічне здоров'я нації. Ключові зусилля України на цьому етапі доречно зосередити на приєднанні до європейських ініціатив загальноєвропейського регулювання соціальних платформ, шукаючи можливість імплементувати в українське законодавство саме діючі європейські норми (наприклад, в межах положень Кодексу практик щодо дезінформації або Акту про цифрові послуги) тощо.

В Україні відсутній законодавчо визначений механізм блокування та видалення деструктивного контенту, поширення якого здійснюється з використанням месенджерів, що унеможлиблює запобігання використанню інформаційного простору у зазначений спосіб на шкоду національній безпеці України, а це якраз відноситься до загроз гібридного типу – різновиду загроз національній безпеці, реалізація яких спричиняє синергетичний ефект від одночасного застосування комбінованих методів впливу, які часто мають прихований характер або маскуються під інші процеси у рамках правового поля. В законодавстві прописано процедури реагування на поширення неправдивої і недостовірної інформації, проте досвід застосування вказаних норм свідчить про чималу кількість недоліків.

Висновки. Результати дослідження вказують на те, що удосконалення вітчизняного інформаційного законодавства є важливим елементом протидії російській інформаційній агресії і загалом можна виокремити дві складові цієї діяльності: перша – це розвиток вітчизняної інформаційної сфери з метою забезпечення участі України як повноправного учасника міжнародного інформаційного обміну, долучення її до європейських ініціатив, друга – це вироблення механізмів протидії проявам інформаційної агресії рф – дезінформації, пропаганді, ІПСО, FIMI тощо.

Пріоритетним напрямом визначено: вироблення дієвих правових механізмів захисту інформаційного суверенітету України, які б забезпечили розвиток українського суспільства в дусі національної гідності, патріотизму та національної свідомості з дотриманням принципів захисту прав, свобод і безпеки людини та законних інтересів суспільства і держави в інформаційній сфері; упорядкування інформаційної діяльності в національному вимірі з метою її ефективної координації на державному рівні, формування національної системи забезпечення інформаційної безпеки, в тому числі побудови ефективної системи стратегічних комунікацій як скоординованої взаємодії органів державної влади з громадянським суспільством; удосконалення комплексу заходів із протидії негативним інформаційним впливам, посилення спроможностей сектору безпеки і оборони щодо протидії спеціальним інформаційним операціям, спрямованим на зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності, підірив обороноздатності України, деморалізацію особового складу Збройних сил України та інших військових формувань, загострення суспільно-політичної ситуації, поширення інформації з обмеженим доступом; посилення юридичної відповідальності суб'єктів українського інформаційного простору, що створені та/або використовуються державою-агресором для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності, зокрема встановлення юридичної відповідальності за умисне систематичне поширення неправдивої інформації, яка створює загрозу суверенітету, територіальній цілісності та недоторканості України, обороноздатності, інформаційній безпеці держави, особливо під час дії правового режиму воєнного стану.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Доронін І.М. Національна безпека України в інформаційну епоху: теоретико-правове дослідження: дис. ... д-ра юрид. наук. Київ, 2020. 539 с.
2. Пилипчук В.Г. Проблема агресії і насильства: світоглядно-інформаційний вимір. URL: <http://socialscience.com.ua/article/806> (дата звернення: 13.05.2025).
3. Корж І.Ф. Вільний доступ громадян до правової інформації – засаднича ознака забезпечення правової безпеки держави. *Інформація і право*. 2018. № 1 (24). С. 14–27.
4. Угода про асоціацію між Україною URL: https://zakon.rada.gov.ua/laws/show/984_011#Text (дата звернення: 14.08.2020).
5. European External Action Service (2021). 2021 StratCom activity report – Strategic Communication Task Forces and Information Analysis Division, available at: https://www.eeas.europa.eu/eeas/2021-stratcomactivity-report-strategic-communication-task-forces-and-information-analysis_en (дата звернення: 24 January 2025).
6. Красноступ Г.М. Нова стратегія інформаційної безпеки: правова відповідь на російське інформаційне маніпулювання та втручання. *Інформація і право*. № 2(53)/2025. С. 136–146.