УДК 342.9:004.056.53:327.8(470:477)
DOI https://doi.org/10.24144/2307-3322.2025.91.3.32

ДО ПИТАННЯ ПРОТИДІЇ НЕГАТИВНОМУ ІНФОРМАЦІЙНОМУ ВПЛИВУ: ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ

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

Солодка О.М. До питання протидії негативному інформаційному впливу: організаційно-правові аспекти.

У статті досліджено, що у сучасному інформаційному суспільстві глобальні трансформації деформують систему інформаційної безпеки та детермінують зміни механізмів її захисту. Руйнування смислової єдності людини і світу – одна з цілей впливу мережевих війн на суспільство, наслідком чого є руйнування базових цінностей народу та держави, національної, культурної ідентичності. Застосовувані технології поширення інструментів інформаційної агресії та стрімкий розвиток цифрового середовища створює суттєві труднощі й вимагає диференціювати критерії шкідливого контенту, що циркулює в медіа середовищі сучасного суспільства, посилити вимоги до суб'єктів, які забезпечують ці процеси.

У статті доведено, що оскільки, інформаційний простір держави є важливим елементом системи забезпечення національної безпеки, ефективна стратегія боротьби з дезінформацією та пропагандою, насамперед, потребує відповідного нормативно-правове забезпечення щодо здійснення таких заходів: створення законодавчої бази для чіткої ідентифікації негативного інформаційного впливу у його проявах – визначення поняття, ознак тощо; створення умов для моніторингу та контент-аналізу інформаційного простору, розробку інструментів моніторингу за допомогою штучного інтелекту, систем оцінювання, систематизації та автоматизації виявлення; медіаконсультацій; або спеціальних програм з протидії; розробки та впровадження механізмів швидкого реагування на дезінформацію, налагодження співпраці відповідними суб'єктами, які є розповсюджувачами такої інформації; визначення координуючого суб'єкта в системі органів державної влади, відповідальних за протидію НІПВ; долучення громадянського суспільства та розвиток державно-приватного партнерства для постійної взаємодії з технологічними компаніями, розроблення організаційно-правових механізмів такої протидії; розвиток освітніх ініціатив із впровадження програм медіа- та інформаційної грамотності у співпраці з міжнародними партнерами, освітніми установами та медіа організаціями; укладення необхідної міжнародної правової основи для ефективної співпраці з зарубіжними партнерами та використання їхнього досвіду боротьби з дезінформацією та пропагандою, забезпечення безпеки інформаційного простору; розвиток інноваційних технологій для виявлення та протидії дезінформації та пропаганди, використання новітніх технологій як штучний інтелект, блокчейн тощо.

Ключові слова: негативний інформаційний вплив, інформаційна безпека, інформаційна агресія, забезпечення інформаційного суверенітету держави.

Solodka O.M. On the issue of countering negative information influence: organizational and legal aspects.

The article explores that in modern information society, global transformations deform the information security system and determine changes in its protection mechanisms. The destruction of the semantic unity of man and the world is one of the goals of the influence of network wars on society, the result of which is the destruction of the basic values of the people and the state, national and cultural identity. The technologies used to disseminate information aggression tools and the rapid development of the digital environment creates significant difficulties and requires differentiating the criteria for harmful content

circulating in the media environment of modern society, and strengthening the requirements for entities that ensure these processes.

The article proves that since the state's information space is an important element of the system of ensuring national security, an effective strategy for combating disinformation and propaganda, first of all, requires appropriate regulatory and legal support for the implementation of the following measures: creating a legislative framework for clear identification of negative information influence in its manifestations – definition of the concept, signs, etc.; creation of conditions for monitoring and content analysis of the information space, development of monitoring tools using artificial intelligence, evaluation systems, systematization and automation of detection; media consultations; or special countermeasure programs; development and implementation of mechanisms of rapid response to disinformation, establishing cooperation between relevant entities that are disseminators of such information; identification of a coordinating entity in the system of state authorities responsible for countering NIPV; involvement of civil society and development of public-private partnerships for constant interaction with technology companies, development of organizational and legal mechanisms for such countermeasures; development of educational initiatives to implement media and information literacy programs in cooperation with international partners, educational institutions and media organizations; establishing the necessary international legal framework for effective cooperation with foreign partners and using their experience in combating disinformation and propaganda, ensuring the security of the information space; developing innovative technologies to detect and counter disinformation and propaganda, using the latest technologies such as artificial intelligence, blockchain, etc.

Key words: negative information influence, information security, information aggression, ensuring the information sovereignty of the state.

Постановка проблеми. Сучасні темпи розвитку інформаційних технологій створили безпрецедентні можливості для розповсюдження інформації, яка поширюється протягом декількох хвилин, не залишаючи можливості для зворотного процесу. Ці обставини стали визначальними для використання інформації у зловмисному впливі, що на сьогодні знайшло відображення у тривалій та інтенсивній інформаційній війні рф проти України. Її основною ідеєю є інформаційний вплив на людину та суспільство з метою регулювання та управління суспільними процесами в глобальному масштабі, що пояснює природу інформаційної агресії. Ця війна призводить до руйнування базових цінностей держави й народу, конфесійної, національної та культурної ідентичності, а ідеологічний та інформаційний вакуум обмежує стратегічний вибір країни в глобалізованому світі, і вона стає частиною системи планетарного контролю [1], для протидії якому необхідне удосконалення як правового, так і організаційного підґрунтя, формування ефективних норм, методик та інструментів протидії дезінформації та розпізнання й недопущення деструктивного інформаційного впливу в умовах перманентної появи

Аналіз останніх досліджень і публікацій. У сучасному науковому дискурсі питання протидії негативним інформаційним проявам та відповідно пошук протидії цьому явищу знайшли відображення у численних наукових працях, зокрема Пилипчука В. [2], Красноступ Г. [3], Стельмаха Д. [4], Курбан О. [5], Кушніра І.П., Адамчука С.В. [6] та інших. Водночас, варто засвідчити, що надшвидкі темпи урізноманітнення інструментів інформаційного впливу формують необхідність удосконалення організаційно-правових засад протидії такому явищу.

Метою статті є визначення напрямів удосконалення організаційно-правових засад протидії негативному інформаційно-психологічному впливу.

Виклад основного матеріалу. У сучасному інформаційному суспільстві глобальні трансформаційні процеси призводять до деформації системи інформаційної безпеки держави та зумовлюють необхідність адаптації механізмів її забезпечення. Однією з ключових цілей інформаційної війни є руйнування фундаментальних цінностей суспільства і держави, спотворення національної та культурної ідентичності, порушення адекватного сприйняття реальності людиною і громадянином. В інформаційній площині гібридні атаки здійснюються через традиційні медіа і соціальні онлайн-мережі, але традиційні методи боротьби з інформаційними атаками в соціальних медіа не дають бажаних результатів. Тому потрібно шукати інші ефективні засоби. На думку О. Курбан, необхідно працювати на випередження, формуючи відповідний рівень критичного мислення в суспільстві [5]. Окрім цього, в умовах появи нових засобів доставки інформації є необхідність у розробці механізмів співпраці з суб'єктами – надавачами таких послуг.

Зокрема, держава має працювати в напрямку врегулювання відносин з Telegram або, у разі відсутності такої можливості та враховуючи ризики, оцінити перспективи заборони його використання на території України. Закон "Про медіа" [7] наділив Нацраду всіма необхідними для комунікації повноваженнями шляхом закріплення її права вести переговори з уповноваженими представниками провайдерів платформ, що не підпадають під юрисдикцію України, та навіть підписувати з ними договори або меморандуми. Окрім цього, є можливість звертатися до іноземних провайдерів платформ щодо обмеження поширення на території України програм та/або користувацької інформації, у тому числі користувацького відео, що порушують вимоги статей 36, 42, 119 Закону. Проте, наявність повноважень Нацради звертатися безпосередньо до Telegram з вимогами щодо обмеження доступу до певної інформації, не означає, що Telegram виконає цю вимогу, адже проблема у питанні комунікації з Telegram та відсутності правил (як національних, так і регіональних), які б могли на практиці врегулювати роботу цього майданчика, так і у відсутності представництва, до якого можна звертатися.

У зазначеному контексті доцільним видається формування експертної групи за участі представників органів державної влади, громадських організацій та кіберсектору з метою обговорення питань правового регулювання діяльності транснаціональних інформаційних суб'єктів, зокрема месенджера Telegram. Важливо забезпечити залучення до цього процесу експертів і представників профільних структур держав-членів ЄС як для запозичення практичного досвіду у сфері регулювання діяльності Telegram, так і для донесення до європейських інституцій інформації про вразливості, що виникають унаслідок його функціонування в умовах воєнного стану. Окремого значення набуває робота над адаптацією законодавства України до норм ЄС у галузі цифрової безпеки та захисту прав користувачів цифрових платформ, зокрема положень Акту про цифрові послуги (DSA). Додатково доцільно розробити рекомендації щодо безпечного використання Telegram, зосередивши особливу увагу на специфіці застосування цього інструменту держслужбовцями та військовослужбовцями.

Зазначені заходи відображають положення Акту про цифрові послуги та Акту про цифрові ринки, відповідно до яких передбачено вплив ЄС як на Інтернет-провайдерів, так і на засновників та власників соцмереж. Оскільки ці акти розповсюджуються на цифрових гігантів, які мають більше 45 мільйонів користувачів на території ЄС (Meta, Apple, Google тощо), Telegram поки що не входить до переліку, адже обсяг користувачів є меншим). Однією з вимог до них є співпраця з національними установами та надання контактної інформації про себе, а також забезпечення прозорості у поширенні інформації, поваги прав своїх користувачів, а деякі навіть мають перебувати під наглядом Європейської комісії – це стосується найбільших онлайн-платформ (Apple AppStore, Booking.com, Facebook, Google Play, Instagram) та пошукових систем (Bing, Google Search), якими користуються понад 10%населення ЄС.

У Digital Services Act та Digital Markets Act [8] відмічено, що хоча платформи і мають певні зобов'язання, втім вони не зобов'язані перевіряти вміст контенту перед публікацією і не відповідатимуть за те, що публікують їхні користувачі, проте негайно реагувати на незаконний контент вони мусять**,** а для цього мають бути створені зрозумілі та доступні інструменти.

Практика іноземних держав теж вказує на вже існуючий досвід у цій сфері. Так, зокрема ухвалюються законодавчі акти з метою блокування та нівелювання небезпечних проявів у мережі Інтернет або у соціальних мережах.

У Великобританії Закон про безпеку в Інтернеті (The Online Safety Act 2023) [9] зобов'язує компанії, що володіють соціальними мережами, забезпечувати безпеку користувачів в онлайн-просторі та дає Регуляторному органу Великобританії Ofcom – Британському офісу комунікацій – повноваження вимагати від технологічних компаній встановлювати системи сканування вмісту кожного повідомлення, хоча учасники ринку переконані, що така вимога може підірвати безпеку та конфіденційність зашифрованих сервісів. Перелік загроз, зафіксований у спеціальному документі під назвою "Online Harms White Paper" [10], поділяється на три категорії: 1) деструктивна інформація, яка має юридичне визначення (пропаганда агресії, заохочення самогубств тощо); 2) шкідлива інформація, яка не має юридичного статусу (тролінг, залякування); 3) легальний контент, не призначений для дітей (ненормативна лексика, додатки сайтів знайомств тощо).

При цьому, як переконливо засвідчує іноземний та міжнародний досвід, ІТ-гіганти, з одного боку, блокують пости та акаунти за власним баченням (оскаржити таке рішення практично неможливо), а з іншого боку – досить часто ігнорують вимоги користувачів або представників влади

тієї чи іншої держави [11] і ця проблематика гостро стоїть на порядку денному ЄС та країн-членів, а для України поглиблюється проблемою використання такої ситуації рф. В цьому контексті доцільним вбачається можливість запровадження спеціального режиму роботи для платформ у період воєнного стану, що передбачає посилені вимоги до фільтрації контенту та видалення інформації, здатної нашкодити національній безпеці держави, яка зазнає агресії, обмеження на поширення інформації з сумнівних джерел та джерел, що розташовані в країнах, визнаних агресорами або недружніми.

Відтак, повномасштабне вторгнення рф ще більше поглибило проблематику забезпечення інформаційної безпеки держави, оскільки засвідчило, що власне інформаційна складова була тією опорною точкою, яка повинна була забезпечити його успіх. Для України це стало новим викликом щодо удосконалення існуючих та формування нових засад вітчизняного інформаційного законодавства. Звісно, що в умовах правового режиму воєнного стану воно має певну специфіку, проте одночасно потребує розробки правових засад унормування інформаційної діяльності відповідних суб'єктів у повоєнний час.

В законодавстві визначено процедури реагування на поширення неправдивої і недостовірної інформації, проте досвід їх застосування свідчить про чималу кількість недоліків. Водночас, закріплені чинним законодавством запобіжні заходи для зловживань та здійснення зовнішнього втручання, практично не регулюють діяльність он-лайн-медіа, соціальних мереж, блогерів, які, в умовах стрімкого розвитку та забезпечення анонімності, найчастіше використовуються для дестабілізації суспільно-політичної ситуації в державі та в інших протиправних цілях. В таких умовах, відповідний суб'єкт не має законних можливостей адекватно реагувати на існуючі загрози в інформаційній сфері. Зазначене свідчить про нагальну потребу законодавчого регулювання національної електронної інформаційної сфери, в т.ч. діяльності соціальних мереж, блогерів, електронних видань та медіа тощо.

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).

Закон України "Про медіа" [7] вперше впроваджує в Україні систему спільного регулювання, яка має на меті збільшити участь самих медіа в розробленні та визначенні вимог до змісту контенту через ухвалення кодексів та забезпечити недопущення цензури й зловживання свободою слова. Ключовим повноваженням органу спільного регулювання є затвердження кодексів (правил) створення та поширення інформації у сферах спільного регулювання та забезпечення механізму надання висновків щодо відповідності інформації, поширеної суб'єктом у сфері медіа, кодексам (правилам) спільного регулювання у випадках виявлення Національною радою ознак можливого порушення таким суб'єктом вимог законодавства та/або умов ліцензії.

Проблемним і досі дискусійним аспектом залишається визначення медійного статусу соціальних платформ. Традиційно компанії, що володіють такими сервісами, позиціонують себе як технічні посередники, які лише забезпечують інфраструктуру для поширення інформації, не втручаючись у її зміст. Відповідно до міжнародних правових актів, така позиція звільняє їх від прямої відповідальності за поширюваний контент. Водночас все більшої актуальності набуває питання: чи не можна розглядати роботу алгоритмів, які формують інформаційну стрічку користувача, як різновид редакційної діяльності. Адже алгоритмічний відбір матеріалів фактично визначає інформаційний порядок денний, впливає на поведінку та сприйняття аудиторії. Якщо визнати цю функцію аналогом редакційної політики, соціальні мережі отримають статус повноцінних медіа і, відповідно, підлягатимуть таким самим регуляторним вимогам, як і традиційні медіа. Проте таке трактування залишається доволі суперечливим і викликає значний науковий та правовий дискурс.

Як уже зазначалось вище, Закон України «Про медіа» [7] наділяє Національну Раду з питань телебачення і радіомовлення повноваженнями у сфері взаємодії з онлайн суб'єктами. На нашу думку, з огляду на розмежування в вітчизняному законодавстві понять інформаційної та кібернетичної безпеки, доцільно розглянути можливість створення національного органу (або визначення серед існуючих установ) на зразок Координатора цифрових послуг (Digital Services Coordinator) – фактично регулятора у сфері діяльності соціальних платформ, через якого можна було б звертатися для вирішення питань ефективного регулювання взаємодії між державою, суспільством, медіа структурами та представниками платформ, розробки спільного регулювання як системи, яка

поєднує елементи державного регулювання та галузевого саморегулювання, забезпечуючи участь суб'єктів (наприклад, цифрових платформ) у розробці правил і вимог, аби уникнути цензури та зловживання свободою для досягнення спільних цілей, наприклад, для забезпечення як якості інформації, так і національної безпеки.

Відтак, нагальність врегулювання питань поширення шкідливого контенту не викликає сумнівів. Разом з тим, вище зазначені заходи можуть уживатися як допоміжні в реалізації стратегічної мети шляхом щодо захисту інформаційного простору України, а саме:

- вироблення дієвих 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, що стало б основою для медіаграмотності суспільства та формування інформаційної культури громадян;
- упорядкування інформаційної діяльності в національному вимірі з метою її ефективної координації на державному рівні, формування національної системи забезпечення інформаційної безпеки, забезпечення моніторингу інформаційного простору, побудови ефективної системи стратегічних комунікацій як скоординованої взаємодії органів державної влади з громадянським суспільством;
- удосконалення комплексу заходів із протидії негативним інформаційним впливам, зокрема шляхом наповнення українського та всесвітнього медіапростору якісним інформаційним продуктом щодо України, просування її іміджу як сильної держави, що має досвід протистояння потужній інформаційній агресії рф;
- створення ефективної системи забезпечення кібернетичної безпеки України, до основних завдань якої віднести: моніторинг кібернетичного простору з метою своєчасного запобігання, виявлення і припинення чи нейтралізації кібернетичних загроз; розроблення відповідної законодавчої бази; кібернетичний захист критичної національної інфраструктури з урахуванням інтересів державно-приватного партнерства.

Висновки. Враховуючи результати здійсненого дослідження, встановлено, що використання новітніх технологій поширення інструментів інформаційної агресії у поєднанні з динамічним розвитком цифрового середовища створює суттєві виклики для захисту інформаційного простору, що зумовлює необхідність розробки ефективної стратегії боротьби з негативними інформаційними впливами, що насамперед, потребує здійснення таких заходів:

1) створення законодавчої бази для чіткої ідентифікації негативного інформаційного впливу у його проявах – визначення поняття, ознак, критеріїв тощо;

2) створення умов для моніторингу та контент-аналізу інформаційного простору, розробку інструментів моніторингу за допомогою штучного інтелекту, систем оцінювання, систематизації та автоматизації виявлення; впровадження медіаконсультацій або спеціальних програм з протидії негативному інформаційному впливу, розробки та впровадження механізмів швидкого реагування на дезінформацію, налагодження співпраці відповідними суб'єктами, які є розповсюджувачами такої інформації;

3) визначення координуючого суб'єкта в системі органів державної влади, відповідальних за протидію негативному інформаційно впливу; долучення громадянського суспільства та розвиток державно-приватного партнерства для постійної взаємодії з технологічними компаніями, розроблення організаційно-правових механізмів такої протидії;

4) розвиток освітніх ініціатив із впровадження програм медіа-, інформаційної та цифрової грамотності у співпраці з міжнародними партнерами, освітніми установами та медіа організаціями.

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) розвиток інноваційних технологій для виявлення та протидії дезінформації та пропаганди, використання новітніх технологій як штучний інтелект, блокчейн тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Contextos Humanistas. Expresiones para el Siglo XXI. Cerdeña: Fondazione Giovannino Pinna, 2022. 90 p.; Getman A.P., Danilyan O.G., Dzeban A.P., Kalynovskyi Yu.Yu. Modern ontology:

reflection on the continuity of cyberspace and virtual reality. *Revista de Filosofía*. 2022. Vol. 39. № 102. P. 78–94.
2. илипчука В. Історико-правові основи становлення і розвитку державності та права в контексті протидії інформаційній та збройній агресії рф проти України. *Інформація і право.* № 3(54)/2025. С. 113–121.
3. Красноступ Г. Правові засади медіаграмотності: від теоретичної концепції до інституціоналізації в державі. *Інформація і право*. № 3(54)/2025. С. 113–121.
4. Стельмах Д. Протидія російським дезінформаційним кампаніям: досвід ЄС. *Інформація і право.* № 2(53)/2025. С. 155–163.
5. Курбан О. Проблема критичності мислення при споживанні медіаконтенту в умовах інформаційної війни. *Синопсис: текст, контент, медіа*. 2022. № 28 (1). С. 21–22.
6. Кушнір І.П., Адамчук С.В. Протидія дезінформації: організаційно-правовий аспект. *Аналітично-порівняльне правознавство*. URL: https://app-journal.in.ua/wp-content/uploads/2025/02/80.pdf (дата звернення: 27.09.2025).
7. Про медіа: Закон України від 13.12.2022 № 2849-IX: URL: https://zakon.rada.gov.ua/laws/show/2849-20 (дата звернення: 27.09.2025).
8. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2022%3A265%3ATOC&uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG (дата звернення: 27.09.2025).
9. Online-safety-act-explainer. URL: https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer (дата звернення: 15.08.2025)
10. Online Harms White Paper. URL: https://assets.publishing.service.gov.uk/media/605e60c6e90e07750810b439/Online_Harms_White_Paper_V2.pdf. (дата звернення: 25.07.2025).
11. Калайда Ю.П. Забезпечення цифрового суверенітету в умовах геополітичного протиборства: кращі практики зарубіжного досвіду. *Інформація і право.* 2021/ № 2(37). С. 145–154.