УДК 342.951:355.02:316.774
DOI https://doi.org/10.32782/klj/2025.2.33

Кравченко В. Г.,
кандидат юридичних наук

МІЖНАРОДНО-ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ МЕХАНІЗМИ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ: ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРАКТИК УКРАЇНИ ТА ЄС

Анотація. У сучасних умовах гібридної війни проти України інформаційний фронт має не менше значення, ніж бойові дії. Загарбники системно використовують методи інформаційної війни, спрямовані на дестабілізацію українського суспільства, підрив довіри до державних інституцій, поширення паніки та послаблення міжнародної підтримки України. Дезінформація, як одна з форм інформаційної агресії, використовується через підконтрольні медіа, соціальні мережі, бот-мережі та анонімні платформи, що значно ускладнює її виявлення та нейтралізацію.

Воєнний стан, запроваджений відповідно до законодавства України, створює підґрунтя для тимчасового обмеження окремих прав і свобод, зокрема права на доступ до інформації та свободи вираження поглядів. Однак такі обмеження мають здійснюватися винятково в межах Конституції України та міжнародних зобов'язань України, з дотриманням принципів необхідності, пропорційності та легітимності. У зв'язку з цим постає нагальна потреба визначення чітких адміністративно-правових меж і засобів втручання держави у сферу інформації, що дозволяють ефективно протидіяти дезінформації без порушення демократичних стандартів.

Застосування організаційно-правових інструментів у боротьбі з дезінформацією включає низку дій: від блокування інформаційних ресурсів і застосування санкцій до регулювання діяльності медіа та реагування на поширення фейкової інформації. Проте на практиці виникають численні виклики, зокрема відсутність уніфікованого визначення дезінформації, розмитість правових критеріїв для її виявлення, ризики зловживання повноваженнями органів виконавчої влади та порушення права на свободу слова. Це потребує детального правового аналізу та доктринального осмислення адміністративно-правового режиму інформаційної безпеки у воєнний період.

Саме тому дослідження організаційно-правових інструментів протидії дезінформації в умовах воєнного стану є надзвичайно актуальним, оскільки дозволяє визначити межі допустимого державного втручання у сферу інформаційних прав, сформувати обґрунтовані підходи до правового регулювання інформаційної безпеки та запобігти порушенню основоположних прав людини навіть у кризовий період.

Ключові слова: *адміністративна відповідальність, інформаційна безпека, дезінформація, воєнний стан, організаційно-правові інструменти, правовий режим, цензура, свобода вираження поглядів, національна безпека, суб'єкти протидії, автоматична фіксація, блокування контенту, інформаційні правопорушення, цифрове регулювання.*

Kravchenko V. H. International legal and organizational mechanisms for countering disinformation: a comparative analysis of the practices of Ukraine and the EU

Abstract. Under the current conditions of hybrid warfare against Ukraine, the information front is no less significant than military operations. The aggressors systematically use methods of information warfare aimed at destabilizing Ukrainian society, undermining trust in state institutions, spreading panic, and weakening international support for Ukraine. Disinformation, as one form of informational aggression, is disseminated through controlled media, social networks, bot systems, and anonymous platforms, which significantly complicates its detection and neutralization.

Martial law, introduced in accordance with Ukrainian legislation, provides a framework for the temporary restriction of certain rights and freedoms, in particular the right to access information and the freedom of expression. However, such restrictions must be carried out strictly within the limits of the Constitution of Ukraine and Ukraine's international obligations, adhering to the principles of necessity, proportionality, and legitimacy. In this regard, there is an urgent need to define clear administrative and legal boundaries and state intervention mechanisms in the information sphere that allow for effective counteraction to disinformation without violating democratic standards.

The application of organizational and legal instruments in the fight against disinformation includes a range of measures: from blocking information resources and imposing sanctions to regulating media activity and

responding to the spread of false information. Nevertheless, numerous challenges arise in practice, including the lack of a unified definition of disinformation, blurred legal criteria for its identification, risks of abuse of power by executive authorities, and violations of freedom of speech. This calls for a detailed legal analysis and doctrinal understanding of the administrative and legal regime of information security during wartime.

Therefore, the study of organizational and legal instruments for countering disinformation under martial law is of utmost relevance, as it helps determine the limits of permissible state intervention in the sphere of information rights, develop substantiated approaches to the legal regulation of information security, and prevent violations of fundamental human rights even during periods of crisis.

Key words*: administrative liability, information security, disinformation, martial law, organizational and legal instruments, legal regime, censorship, freedom of expression, national security, counteraction actors, automated detection, content blocking, information offenses, digital regulation.*

Постановка проблеми. Ескалація гібридної війни актуалізувала потребу в ефективних механізмах протидії інформаційним загрозам. Одним із найнебезпечніших проявів таких загроз є дезінформація, що підриває інформаційну безпеку держави. Існуючі організаційно-правові засоби боротьби з нею залишаються фрагментарними та недостатньо ефективними. Законодавство не містить єдиного підходу до визначення дезінформації, а компетенції уповноважених органів часто дублюються або залишаються розмитими. Водночас зростає ризик надмірного втручання держави в інформаційний простір, що може загрожувати конституційним правам людини. Це зумовлює необхідність доктринального уточнення меж і форм організаційно-правового реагування в умовах воєнного стану.

Огляд літератури свідчить про зростаючий інтерес до дезінформації як загрози безпеці. Цей феномен розглядається у працях О. Бучковської, Ю. Горбаня, О. Олійник, О. Горуна, Б. Гривнака, І. Лопушинського, І. Сапіжака, О. Звоздецької, А. Марущака, О. Панченка, В. Антонова, Л. Рудник, Ю. Синиціної, С. Федоренка, Т. Павленко, Т. Шлемкевич та інших. Водночас, комплексне дослідження організаційно-правових аспектів протидії дезінформації в умовах воєнного стану в українському науковому просторі наразі відсутнє.

Виклад основного матеріалу. Розвиток цифрових технологій суттєво трансформував усі сфери суспільного життя, включаючи правову систему, публічне адміністрування, економіку, освіту тощо. На перший погляд, загальна доступність інформаційного простору та можливість кожного громадянина створювати і поширювати контент є важливим кроком у реалізації базових прав і свобод людини, насамперед – права на свободу вираження поглядів і права на доступ до інформації. Проте за цими позитивними здобутками приховується низка ризиків, що мають як індивідуальний, так і загальнодержавний характер, особливо в умовах венного стану, коли держава стримує військовий напад від найближчих «сусідів-ворогів».

У цифровому середовищі спостерігається надмірне насичення інформаційного простору, при якому істотно ускладнюється розрізнення достовірної інформації від хибної або маніпулятивної. Сучасні технології дозволяють не лише оперативно поширювати повідомлення, але й цілеспрямовано конструювати фальсифіковану реальність – через фейки, діпфейки, перекручування фактів або навмисне зміщення акцентів. Такі дії можуть бути вчинені як свідомо – з пропагандистською, політичною або економічною метою, так і несвідомо – через необізнаність, недбалість або навіть з переконанням про «благі наміри».

Особливої загрози набуває ситуація, коли дезінформація поширюється як в онлайн-просторі (через соціальні мережі, месенджери, відеохостинги, анонімні канали), так і офлайн – у вигляді роздрукованих матеріалів, публічних виступів або міжособистісного спілкування. Нерідко зміст таких повідомлень набуває форми напівправди або змішаних фактів, що ускладнює правове реагування і викликає недовіру до офіційної інформації. Маніпуляція смислами, термінами, візуальними образами, емоційними тригерами – все це призводить до викривлення уявлень про реальність у значної частини населення, що в умовах війни може мати критичні наслідки для національної безпеки.

Сучасне правове регулювання інформаційної безпеки в Україні базується на низці нормативно-правових актів, які встановлюють загальні засади обігу інформації, визначають компетенцію органів державної влади у сфері інформаційної політики та закріплюють правові механізми захисту національного інформаційного простору, особливо в умовах дії особливих правових режимів, зокрема воєнного стану. Водночас вартим уваги є той факт, що наявна законодавча база є фрагментарною, оскільки не забезпечує належного реагування на системну інформаційну загрозу – дезінформацію, що активно використовується у сучасних умовах гібридної війни. Зокрема, Конституція України від 28 червня 1996 року № 254к/96-ВР гарантує право на свободу слова (стаття 34), а також передбачає можливість тимчасового обмеження прав і свобод громадян під час воєнного або надзвичайного стану (ст. 64). Таким чином, закріплюється правовий фундамент для нормативного втручання у сферу інформаційних відносин з метою забезпечення національної безпеки. Закон України «Про правовий режим воєнного стану» від 12 травня 2015 року № 389-VIII визначає порядок реалізації публічної влади в умовах воєнного стану, зокрема, передбачає можливість обмеження діяльності засобів масової інформації, встановлення особливих правил поширення інформації, а також здійснення державного контролю за її змістом. Водночас цей закон не містить чітких орієнтирів щодо кваліфікації та ідентифікації дезінформації як окремого виду правопорушення.

Закон України «Про інформацію» від 2 жовтня 1992 року № 2657-XII визначає базові терміни, такі як «інформація», «неправдива інформація», «інформаційна безпека», однак не містить легальної дефініції дезінформації, не розкриває її ознак, мети поширення або специфіки впливу на суспільну свідомість. Аналогічно, Закон України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII визначає інформаційну безпеку як одну зі складових національної безпеки та покладає на державу обов'язок протидіяти інформаційним загрозам, однак також не містить інструментально-прикладного регламенту щодо дезінформації як загрози публічному порядку чи інституційній стійкості держави.

Закон України «Про телебачення і радіомовлення» від 21 грудня 1993 року № 3759-XII та Закон України «Про Національну раду України з питань телебачення і радіомовлення» від 23 вересня 1997 року № 538/97-ВР надають регулятору широкі повноваження щодо моніторингу змісту медіа, застосування санкцій, призупинення дії ліцензій тощо, однак їхні положення також не містять чіткого критеріального апарату для визначення інформації як дезінформаційної.

Постанова Кабінету Міністрів України № 866 від 6 жовтня 2021 року «Про затвердження Порядку функціонування системи інформування населення під час особливого періоду та в разі виникнення кризової ситуації» регламентує лише технічні й організаційні аспекти поширення офіційної інформації, не зачіпаючи при цьому питань протидії дезінформації.

Таким чином, незважаючи на наявність широкого масиву нормативних актів, в Україні на сьогодні відсутнє нормативно встановлене поняття «дезінформація», не визначено її ключові ознаки, специфіка, види, мета поширення та правовий механізм виявлення й реагування. Такий дефінітивний вакуум створює підґрунтя для довільного трактування інформаційної діяльності з боку уповноважених органів, що в умовах воєнного стану може призводити як до правових зловживань, так і до безкарності ворожих інформаційних операцій. У цьому контексті особливої ваги набувають напрацювання міжнародної наукової доктрини, що пропонують аналітичні моделі для диференціації дезінформації та суміжних категорій.

Так, у межах дослідження для Ради Європи 2017 року, підготовленого Клер Уордл та Хосейном Дарахшаном, була запропонована трикомпонентна класифікація форм проблемного контенту в інформаційному середовищі, яка базується на критеріях наміру, точності й потенційної шкоди. Згідно з цією моделлю, виділяються три ключові категорії: по-перше, дезінформація (disinformation) – це свідомо неправдива інформація, яка створю-

ється і поширюється з метою завдання шкоди окремій особі, соціальній групі, інституції або державі; по-друге, неправдива інформація (misinformation) – помилкова, але поширена без наміру нашкодити; по-третє, спотворена інформація (malinformation) – достовірна за формою, але вирвана з контексту або використана маніпулятивно з метою завдати шкоди (наприклад, поширення особистої інформації чи конфіденційних даних).

Цей підхід дозволяє враховувати не лише зміст повідомлення, але й суб'єктивну складову – тобто наявність або відсутність умислу, який і є принциповою відмінністю між дезінформацією та іншими формами недостовірного контенту. Наприклад, пересічний користувач соціальних мереж, що поширює помилково підписане відео або сатиричний контент, сприйнятий як реальний, не є джерелом дезінформації в юридичному сенсі. Така особа, хоч і розповсюджує неправду, не має наміру ввести в оману – отже, йдеться про misinformation. Натомість дезінформація передбачає не лише фактичну неправдивість повідомлення, але й завідомий умисел на спотворення реальності в інтересах певного суб'єкта.

Аналогічну типологію містить Кодекс ЄС з протидії дезінформації, який визначає дезінформацію як підтверджено хибну чи оманливу інформацію, створену, подану або поширену з метою економічної вигоди або навмисного введення громадськості в оману, яка водночас може призвести до шкоди публічним інтересам – таким як демократичні процеси, суспільне здоров'я, екологічна безпека, національна оборона тощо. Окремо вказано, що до дезінформації не належать сатира, пародія, редакційні помилки, політичні коментарі, а також чітко марковані суб'єктивні оцінки.

До схожих висновків приходить і спеціальна доповідачка ООН Ірен Хан у своєму звіті 2021 року, присвяченому взаємозв'язку дезінформації та свободи вираження поглядів. У цьому документі дезінформація визначається як навмисне поширення неправдивої інформації з метою спричинення серйозної суспільної шкоди, тоді як misinformation – це неусвідомлене розповсюдження помилкових повідомлень, що не має злого умислу.

Загальновизнаною в науковому дискурсі вважається також позиція, згідно з якою дезінформація має щонайменше три обов'язкові елементи: спотворений або повністю вигаданий зміст повідомлення, який не відповідає дійсності; умисел суб'єкта поширення на введення в оману; мета вплинути на поведінку, сприйняття чи рішення адресата.

Показово, що навіть у тлумаченнях українських словників поняття «дезінформація» трактується як свідоме поширення неправдивої інформації з метою ввести в оману громадську думку, досягти антигуманної або маніпулятивної мети.

У науковій літературі цей підхід підтримують, зокрема, Ю. Синиціна та С. Федоренко, які розглядають дезінформацію як поширення неправдивої або маніпульованої інформації з метою впливу на громадську думку. В той же час Л.І. Рудник підкреслює, що ключовою ознакою дезінформації, яка відрізняє її від звичайної недостовірної інформації є умисел на її створення, якщо умислу не було, то йдеться про неперевірену інформацію, яка виявилася недостовірною.

У 2020 році Міністерством культури, молоді та спорту України було презентовано законопроєкт «Про протидію дезінформації», в якому, попри його подальше відкликання, вперше на нормативному рівні запропоновано визначення цього явища як недостовірної інформації з питань, що становлять суспільний інтерес, насамперед щодо національної безпеки, суверенітету, оборони, права на самовизначення, охорони здоров'я та навколишнього середовища. Ця концепція передбачала запровадження спеціального механізму спростування дезінформації, обов'язок маркування джерел, створення посади Уповноваженого з питань інформації, проте так і не була реалізована.

Таким чином, наявні теоретичні напрацювання дозволяють зробити обґрунтовану спробу авторського визначення досліджуваного явища. На нашу думку, **дезінформація –** *це цілеспрямовано створена або поширена недостовірна інформація, що подається як достовірна з метою введення в оману конкретної аудиторії та досягнення політичної, економічної, соціальної або іншої вигоди,*

яка має потенціал спричинення суспільної шкоди.

У світлі цього визначення доцільно окреслити найбільш поширені форми та види дезінформації, які функціонують в інформаційному просторі, зокрема в контексті гібридної агресії проти України.

До основних форм поширення дезінформації належать: пропаганда – цілеспрямоване поширення інформації, ідей або чуток з метою формування певного емоційного чи когнітивного впливу на масову свідомість, зазвичай в інтересах політичних суб'єктів або держав. У більшості випадків має політично-ідеологічне спрямування і використовується для делегітимації опонента або посилення впливу власної позиції; фейк – повністю вигадана інформація, що маскується під достовірне повідомлення. Поширюється через імітацію структури новинних сайтів, фальшиві акаунти, фіктивні аналітичні портали, що вводить в оману навіть критично налаштованих споживачів; діпфейк (англ. deepfake) – це штучно створений або змінений за допомогою технологій штучного інтелекту (особливо глибокого навчання, deep learning) аудіо- чи відеоконтент, який імітує реальну людину – її обличчя, голос, міміку або поведінку – з високим ступенем правдоподібності, але містить сфабриковану інформацію; «джинса» – платні або контрольовані державними чи політичними структурами публікації, що подаються під виглядом незалежної журналістики. Їх метою є маніпуляція громадською думкою, підміна реального змісту публічних дискусій; упереджені новини – контент, який експлуатує вже сформовані переконання або стереотипи аудиторії, підсилюючи її власні упередження та запобігаючи критичному осмисленню альтернативних точок зору; сатира – створення навмисно неправдивих або гротескних повідомлень із метою розваги або іронічної критики, однак у деяких випадках вона сприймається як достовірна, що може стати джерелом поширення хибних уявлень; клікбейт – подача перебільшених або оманливих заголовків, зображень чи описів, які провокують користувача на перехід до матеріалу, часто безвідносно до його реального змісту, з метою штучного створення трафіку.

У цьому контексті особливе значення має унормування ключових термінів, які використовуються у правозастосовній практиці, зокрема таких як «дезінформація», «маніпулятивна інформація», «фейк», «мізінформація», «діпфейк» тощо. Ці терміни мають бути чітко зафіксовані у базовому законодавчому акті – Законі України «Про інформацію» від 2 жовтня 1992 року № 2657-XII – з метою усунення правової невизначеності, уніфікації тлумачень і запобігання зловживанням при кваліфікації відповідних дій

У межах класифікації видів дезінформації, відповідно до мети її поширення, виокремлюють:

1. Маніпуляцію – вплив на емоційний або раціональний рівень сприйняття аудиторії з використанням напівправди, вирваних з контексту цитат, недостовірних посилань.

2. Обман конкретної особи чи групи осіб – адресна дезінформація, що спрямована на дискредитацію, формування хибного образу, нав'язування певних рішень або вчинків.

3. Формування суспільної думки – довготривалі інформаційні кампанії, спрямовані на зміну ціннісних орієнтацій, політичної лояльності, національної ідентичності.

Окремо слід наголосити на тому, що ненавмисне поширення недостовірної інформації, так звану мізінформацію (misinformation), не можна ототожнювати з дезінформацією через відсутність умислу. Проте в умовах гібридної війни навіть неусвідомлене тиражування помилкових повідомлень може мати руйнівні наслідки, особливо коли йдеться про інформацію, пов'язану з безпекою, війною, здоров'ям чи міжнародною політикою.

Для кваліфікації інформації як дезінформації доцільно орієнтуватися на комплекс об'єктивних та суб'єктивних ознак, до яких належать:

– свідомий умисел поширювача або замовника на спотворення реальності;

– наявність суспільно важливої тематики (безпека, здоров'я, вибори, війна, публічний порядок тощо);

– структурна неправдивість повідомлення, що може проявлятися як у повному вигадуванні фактів, так і в монтажі реальних відомостей у маніпулятивний спосіб;

– імітація достовірності: подання неправдивої інформації у формах, типовим для легітимних джерел (новини, офіційні звіти, експертні коментарі);

– шкода або ризик її спричинення, яка може виражатися в підриві суспільної довіри, масових порушеннях громадського порядку, дискредитації інституцій тощо;

– використання механізмів масового охоплення (зокрема, через цифрові платформи, мережі ботів, анонімні ресурси);

– зв'язок із політичними, ідеологічними або геополітичними цілями.

Отже, відмежування дезінформації від суміжних явищ – це передусім питання правової точності та безпекової необхідності.

У межах організаційно-правового механізму протидії дезінформації в Україні важливу роль відіграють органи публічної влади, уповноважені на реалізацію інформаційної політики, безпеки у цифровому середовищі, контролю за засобами масової інформації та забезпеченням національного інформаційного суверенітету. Однак нормативно-правова база, що регулює розподіл повноважень між цими суб'єктами, характеризується фрагментарністю, нечіткістю функціонального наповнення та відсутністю координаційного центру.

Центральне місце у системі органів, що відповідають за реалізацію державної інформаційної політики, посідає Міністерство культури та інформаційної політики України. Відповідно до Положення, затвердженого постановою Кабінету Міністрів України від 16 жовтня 2019 р. № 885, міністерство формує та реалізує державну політику у сфері інформаційного суверенітету, стратегічних комунікацій, інформаційної безпеки, розвитку медіа та протидії дезінформаційним загрозам. Водночас, на практиці цей орган не має спеціалізованих інструментів виявлення та блокування дезінформації, а його повноваження обмежені переважно формуванням нормативної та комунікаційної політики. Відсутність механізмів оперативного реагування та санкціонування свідчить про необхідність розширення адміністративного мандату цього органу.

Національна рада України з питань телебачення і радіомовлення є конституційним незалежним органом, створеним відповідно до Закону України «Про Національну раду України з питань телебачення і радіомовлення» від 23 вересня 1997 року № 538/97-ВР. Національна рада України має повноваження щодо моніторингу медіаконтенту, застосування санкцій до телерадіоорганізацій, видачі та анулювання ліцензій, а також звернення до суду у разі виявлення порушень законодавства у сфері інформаційної діяльності. Проте чинне законодавство не визнає дезінформацію як окрему правову категорію, що значно ускладнює правозастосування з боку Національної ради України та створює прогалину в інструментарії організаційно-правового реагування.

Служба безпеки України, керуючись Законом України «Про Службу безпеки України» від 25 березня 1992 року № 2229-XII, здійснює заходи із захисту державного суверенітету, у тому числі в інформаційному просторі. На практиці саме Служба ініціює блокування вебресурсів, викриття агентур мереж, притягнення до відповідальності осіб, причетних до поширення дезінформації. Проте така діяльність здебільшого реалізується у межах кримінально-правового механізму, що не дозволяє належно оцінити потенціал організаційно-правових засобів впливу в цій сфері. Відсутність формалізованих процедур адміністративного реагування свідчить про потребу у правовій деталізації відповідних інструментів.

Національна поліція України, діючи відповідно до Закону України «Про Національну поліцію» від 2 липня 2015 року № 580-VIII, уповноважена забезпечувати публічний порядок, захист прав і свобод громадян, у тому числі в цифровому середовищі. Однак, незважаючи на наявність технічних і ресурсних можливостей, поліція не має прямих повноважень щодо виявлення та блокування дезінформації як окремої категорії інформаційного правопорушення. Її діяльність обмежена складанням адміністративних протоколів та співпрацею з іншими органами. Це вказує на необхідність нормативного доопрацювання адміністративної компетенції поліції в інформаційній сфері.

Державна служба спеціального зв'язку та захисту інформації України, відповідно

до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23 лютого 2006 року № 3475-IV, відповідає за криптографічний захист, кібербезпеку державних інформаційних ресурсів та координацію у сфері телекомунікацій. Безпосереднє реагування на дезінформаційні кампанії не входить до переліку її повноважень, однак служба забезпечує функціонування технічної інфраструктури держави та бере участь у реалізації загальнодержавних заходів кіберзахисту.

У структурі цієї служби функціонує також Національний центр оперативно-технічного управління мережами телекомунікацій. Центр було створено у 2019 році. Його завданням є оперативно-технічне управління електронними комунікаційними мережами всіх постачальників під час надзвичайних ситуацій, надзвичайного або воєнного стану.

Центр забезпечує централізоване управління мережами телекомунікацій у кризових ситуаціях, зокрема під час воєнного стану або при виникненні загроз національній безпеці. Він виконує функції технічного координатора з реалізації рішень уповноважених суб'єктів щодо обмеження доступу до окремих інформаційних ресурсів. Проте Центр не має адміністративно-юрисдикційних повноважень і не може самостійно оцінювати або кваліфікувати зміст інформації як дезінформаційний. Це визначає його роль як технічно-виконавчого, а не правозастосовного органу.

Відповідну постанову ухвалив Кабінет Міністрів України, якою затверджено Порядок створення та діяльності системи оперативно-технічного управління електронними комунікаційними мережами загального користування та Національного центру оперативно-технічного управління електронними комунікаційними мережами України в умовах надзвичайної ситуації, надзвичайного або воєнного стану (постанова від 24 січня 2025 року № 75).

До складу цієї системи входять: Адміністрація Державної служби спеціального зв'язку та захисту інформації України як головний орган управління, Національний центр оперативно-технічного управління електронними комунікаційними мережами, центри управління мережами, які є структурними підрозділами постачальників електронних комунікаційних послуг, що виконують функції безпосереднього управління власними мережами, а також інформаційно-аналітична система оперативно-технічного управління та відповідні технічні засоби.

Постанова розроблена з урахуванням досвіду організації мереж електронних комунікацій під час воєнних дій. Вона має на меті унормування нормативно-правової бази відповідно до вимог Єдиного цифрового ринку Європейського Союзу та приведення її у відповідність до Закону України «Про електронні комунікації», а також до сучасних викликів у сфері безпеки.

Окрім оновлення складу системи, зазначений Порядок визначає принципи функціонування системи в умовах звичайного та надзвичайного режимів, підготовку електронних комунікацій загального користування до функціонування в умовах надзвичайного або воєнного стану, взаємодію складових системи оперативно-технічного управління з підрозділами Збройних Сил України, інших військових формувань та правоохоронних органів. Також встановлено повноваження Національного центру оперативно-технічного управління електронними комунікаційними мережами щодо тимчасового обмеження надання електронних комунікаційних послуг у цілях оборони та безпеки держави.

Зі зростанням усвідомлення загроз, які несе дезінформація для державного суверенітету, національної безпеки, громадської стабільності та міжнародного авторитету України, питання запровадження ефективних механізмів відповідальності за її поширення набуває дедалі більшої актуальності. У реаліях повномасштабної війни проти України, інформаційний фронт перетворився на ключовий напрямок гібридної агресії, в межах якого дезінформація використовується як інструмент руйнування єдності суспільства, послаблення довіри до держави, деморалізації військовослужбовців, створення хаосу та провокацій серед цивільного населення. Тому обов'язок держави – не лише ідентифікувати такі загрози, але й належно реагувати на них засобами правового характеру, забезпечуючи

баланс між захистом національної безпеки та гарантуванням прав і свобод громадян.

В умовах воєнного стану Україна дійсно активізувала інструменти впливу на інформаційне середовище. Так, на підставі рішень Ради національної безпеки і оборони України, введених у дію указами Президента України, до окремих фізичних осіб, включаючи інтернет-блогерів, журналістів та так званих «лідерів громадської думки», застосовуються персональні спеціальні економічні та інші обмежувальні заходи (санкції). Це стосується, зокрема, осіб, які свідомо поширюють ворожі наративи, транслюють ідеологію «русского міра», заперечують факт російської агресії чи дискредитують українські Збройні Сили. Застосування санкцій щодо таких суб'єктів у межах воєнного стану є виправданим, коли мова йде про іноземних громадян або про тих, хто діє в інтересах держави-агресора.

Однак варто підкреслити, що механізм санкцій, як позасудовий інструмент реагування, не повинен підміняти собою систему юридичної відповідальності. Особливо це актуально щодо громадян України – навіть якщо їхні дії несуть деструктивний характер. Притягнення до відповідальності таких осіб повинно здійснюватися за встановленою процедурою: через складання процесуальних документів, відкриття адміністративного або кримінального провадження, розгляд справи в суді, ухвалення законного та обґрунтованого рішення. Лише в такому разі буде дотримано принцип верховенства права, презумпції невинуватості та права на захист. Застосування санкцій до громадян України без судового розгляду або належної процедури створює загрозу порушення конституційних прав та викликає сумніви в легітимності державного реагування.

Треба зазначити, що чинне законодавство України вже містить низку положень, які можуть бути використані для правової протидії поширенню дезінформації. Зокрема, Кодекс України про адміністративні правопорушення передбачає відповідальність за поширювання неправдивих чуток, які можуть викликати паніку або дестабілізувати громадський порядок – стаття 173-1 («Поширювання неправдивих чуток»). Це положення застосовується у разі розповсюдження інформації без підтвердження джерела, яка провокує суспільне занепокоєння або дезорієнтацію. Адміністративна відповідальність також можлива за порушення порядку розповсюдження інформації у ЗМІ, зокрема відповідно до статті 212-3 КУпАП.

У Кримінальному кодексі України існує низка положень, що дозволяють притягати до кримінальної відповідальності осіб, дії яких мають дезінформаційний або інформаційно-диверсійний характер. Наприклад, стаття 111-1 передбачає покарання за колабораційну діяльність, що включає інформаційну співпрацю з державою-агресором. Крім того, стаття 114-2 визначає кримінальну відповідальність за несанкціоноване поширення інформації про переміщення чи розташування Збройних Сил України в умовах воєнного або надзвичайного стану. У комплексі ці статті спрямовані на запобігання підриву обороноздатності держави в інформаційному аспекті.

Окремі положення щодо санкційної політики містяться у Законах України «Про санкції» від 14 серпня 2014 року № 1644-VII та «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII. Вони надають можливість застосовувати персональні обмежувальні заходи до осіб, що становлять загрозу інформаційній безпеці або вчиняють деструктивну діяльність на користь держави-агресора. Проте ці заходи мають використовуватися лише щодо іноземців або громадян, які втратили зв'язок із Україною де-факто. До громадян України, що проживають на території, підконтрольній державі, такі заходи мають застосовуватись виключно за рішенням суду, із дотриманням принципу правової визначеності.

Висновки. З огляду на виклики, що постають перед державою в умовах збройної агресії та інформаційної війни, зростає потреба у створенні цілісної та ефективної системи організаційно-правових заходів протидії дезінформації. Важливо, щоб така система не лише забезпечувала реагування на факти поширення недостовірної чи маніпулятивної інформації, але й ґрунтувалася на принципах верховенства права, правової визначеності та відповідності міжнародним стан-

дартам у сфері прав людини. Забезпечення ефективної комунікації між органами державної влади, чіткий розподіл повноважень і розвиток нормативно-правової бази мають стати основою для формування довготривалої інформаційної політики держави, здатної ефективно протистояти викликам гібридної війни.

Отже, ефективна протидія дезінформації можлива лише за умови гармонізації правового інструментарію, його відповідності стандартам верховенства права та забезпечення балансу між безпекою та свободою в умовах особливого правового режиму. Водночас важливо, щоб будь-яке нормативне втручання в інформаційний простір не перетворювалося на інструмент цензури чи політичного переслідування. Усі дії держави мають відповідати принципам правової визначеності, відкритості процесів і захисту основоположних прав людини, навіть за умов воєнного стану. Розбудова ефективної системи протидії дезінформації повинна спиратися на чітко окреслені межі втручання, відповідальність уповноважених суб'єктів та механізми громадського і судового контролю.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Конституція України від 28 червня 1996 року № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141.

2. Про правовий режим воєнного стану: Закон України від 12 травня 2015 року № 389-VIII. Відомості Верховної Ради України. 2015. № 28. Ст. 250.

3. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XI. Відомості Верховної Ради України. 1992. № 48. Ст. 650.

4. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. Відомості Верховної Ради України. 2018. № 31. Ст. 241.

5. Про телебачення і радіомовлення: Закон України від 21 грудня 1993 року № 3759-XI. Відомості Верховної Ради України. 1994. № 10. Ст. 43.

6. Про Національну раду України з питань телебачення і радіомовлення: Закон України від 23 вересня 1997 року № 538/97-ВР. Відомості Верховної Ради України. 1997. № 48. Ст. 296.

7. OSCE Representative on Freedom of the Media. Joint declaration on freedom of expression and «fake news», disinformation and propaganda. 3 March 2017. URL: https://www.osce.org/files/f/documents/6/8/302796.pdf

8. Wardle C., Derakhshan H. Information Disorder: Toward an interdisciplinary framework for research and policy making. 2nd edition. Strasbourg: Council of Europe, 2018. URL: https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77

9. EU Code of Practice on Disinformation. URL: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

10. Khan I. Disinformation and freedom of opinion and expression: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. 2021. UN Doc. A/HRC/47/25. URL: https://undocs.org/A/HRC/47/25

11. Дворовий М., Людва А. Протидія дезінформації в інтернеті: куди рухатися Україні? Грудень 2021. URL: https://www.nrada.gov.ua/wp-content/uploads/2022/02/DSLU_Disinformation_Ukraine_Report.pdf

12. Синиціна Ю., Федоренко С. Можливості та виклики штучного інтелекту та виявлення дезінформації: мат. VIII міжн. наук.-практ. конф. (м. Дніпропетровський державний університет внутрішніх справ, 15 березня 2024 року). Частина II. С. 391–392.

13. Рудник Л.І. Поширення недостовірної інформації як засіб ведення гібридних війн. *Інформація і право*. 2024. № 4(51). С. 46–54.

14. Про протидію дезінформації. Презентація закону. URL: https://mkip.gov.ua/files/InformPolityka.pdf

15. Положення про Міністерство культури та стратегічних комунікацій України: затв. постановою Кабінету Міністрів України від 16 жовтня 2019 року № 885. URL: https://zakon.rada.gov.ua/laws/show/885-2019-%D0%BF#Text

16. Про Службу безпеки України: Закон України від 25 березня 1992 року № 2229-XII. Відомості Верховної Ради України. 1992. № 27. Ст. 382.

17. Про Національну поліцію: Закон України від 2 липня 2015 року № 580-VIII. Відомості Верховної Ради України. 2015. № 40. Ст. 379.

18. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23 лютого 2006 року № 3475-IV. Відомості Верховної Ради України. 2006. № 30. Ст. 258.

19. Порядок створення та діяльності системи оперативно-технічного управління електронними комунікаційними мережами загального користування та Національного центру оперативно-технічного управління електронними комунікаційними мережами України в умовах надзвичайної ситуації, надзвичайного або воєнного стану: затверджено постановою Кабінету Міністрів України від 24 січня 2025 року № 75. URL: https://zakon.rada.gov.ua/laws/show/75-2025-%D0%BF#n10

20. Кодекс України про адміністративні правопорушення: Кодекс України від 7 грудня 1984 року № 8073-X. Відомості Верховної Ради Української РСР. 1984. Додаток до № 51. Ст. 1122.

21. Кримінальний процесуальний кодекс України: Кодекс України від 13 квітня 2012 року № 4651-VI. Відомості Верховної Ради України. 2013. № 9–10. Ст. 88.

22. Про санкції: Закон України від 14 серпня 2014 року № 1644-VII. Відомості Верховної Ради України. 2014. № 40–41. Ст. 2021.