DOI: 10.18372/2307-9061.64.16897
УДК 343.33(045)

І. М. Сопілко,
доктор юридичних наук, професор
ORCID ID: https://orcid.org/0000-0002-9594-9280

ІНФОРМАЦІЙНА ВІЙНА ПРОТИ УКРАЇНИ ТА ПРАВОВІ ЗАСОБИ ПРОТИДІЇ ЗЛОЧИННИМ ДІЯМ

Національний авіаційний університет
проспект Любомира Гузара, 1, 03680, Київ, Україна
E-mail: sopilko_i@ukr.net

Мета: *дослідити особливості та сутність інформаційної війни та надати рекомендації з приводу правового регулювання відповідних питань в Україні.* ***Методи дослідження:*** *дана наукова стаття була написана автором із залученням загальновизнаних методів наукового пізнання, а саме, аналітичного, формального, порівняльно-правового, системно-структурного та інших.* ***Результати:*** *досліджено поняття, суть, характеристики інформаційної війни та пов'язаних із нею категорій, вказано на проблеми забезпечення протидії зловимсним діям у цій сфері, надано пропозиції щодо подолання таких проблем шляхом вдосконалення чинного законодавства, в тому числі, за рахунок досвіду інших країн та гармонізації діючої нормативно-правової бази із стандартами Євросоюзу.* ***Обговорення:*** *дискусія у науковому дослідженні ведеться щодо особливостей правового врегулювання загроз та ризиків, з якими стикається Україна під час гібридної та безпосередньо інформаційної війни, що ведеться проти неї.*

Ключові слова: *інформаційна війна; інформаційна безпека; кібервійна; гібридна війна; національна безпека.*

Постановка проблеми та її актуальність. Як відомо, Україна вже давно була втягнута у гібридну війну, невід'ємним елементом якої є війна інформаційна. У контексті останньої також вирізняється кібернетична війна. Взагалі спроби впливати на свідомість окремих індивідів і навіть цілих соціальних груп за допомогою інформації відомі з моменту виникнення людської раси, про що говорять усталені традиції та стереотипи. Хоча саме про інформаційну війну в сьогоднішньому розумінні тоді, звичайно, не йшлося. Але на даному етапі людського розвитку, коли використання інформаційних мереж стало невід'ємним елементом щоденної взаємодії, саме інформаційна зброя стала основним інструментом та рушійною силою серед світових владних суб'єктів.

Понад вісім років проти України Російською Федерацією ведеться гібридна війна. У лютому 2022 року Росія почала безжально вбивати мирних українських жителів, бомбардувати об'єкти невоєнного призначення, а також іншими способами порушувати норми та підвалини міжнародного права взагалі та міжнародного гуманітарного права зокрема. При цьому з не меншим розлюченням країна-агресор намагається справити інформаційний вплив як на громадян України за допомогою вкидання фейків та пропаганди, так і на власний народ, помістивши його у інформаційний вакуум. Мають місце спроби противника отримати контроль над засобами передачі інформації, особливо це стосується Всесвітньої Мережі Інтернет. Метою таких дій є змусити людей мислити бажаним для ворога способом, нав'язати жертвам свої цілі та принципи.

Саме тому важливо знати, що таке інформаційна війна, не менш цінним для кожного українця буде й розуміння того, як протидіяти агресивним діям противника в інформаційному

просторі. Детальне ознайомлення із правовими методами протидії незаконній активності у ході інформаційної війни допоможе українцям захистити свої інформаційні права та інтереси. Про це й піде мова у данному науковому дослідженні.

Аналіз досліджень і публікацій з проблеми. Цій проблемі були присвячені роботи таких вітчизняних науковців: Л. Бєлкін, М. Бучин, О. Курбан, Ю. Курус, Ю. Юринець, В. Філінович та інших.

Мета статті. Автор даної наукової роботи ставить собі за мету розкрити суть і особливості поняття «інформаційна війна» та інших, пов'язаних із ним термінів, зробити їх порівняльно-правовий аналіз, запропонувати набір рекомендацій щодо удосконалення діючого заонодавства та подолання безпосередніх прогалин у правовому регулюванні відповідних питань.

Виклад основного матеріалу. Інформатизація сьогодні – це те, без чого наше існування вже немислиме. Ефективне використання, накопичення, передача даних із застосуванням інформаційних технологій тощо – все це робить з українського народу справжнє інформаційне суспільство. Але ця сама інформатизація справила і негативний вплив, зокрема, вказане виявилося у розгортанні інформаційних воєн проти нашої суверенної держави. Як зазначає Ю.Л. Юринець, Л.М. Бєлкін та інші вчені, небажаний культурний зміст та утилітарні цінності набули широкого поширення саме завдяки диджиталізації. Зазначене суттєво вплинуло на формування спотвореної авторитарно-орієнтованої системи цінностей замість гуманістично-ліберальної і на рівні окремих осіб, і на національному рівні [1, с. 25].

Як уже було зазначено вище, для української держави тема інформаційного протистояння набула особливої актуальності в останнє десятиліття у зв'язку з агресією та веденням проти неї гібридної війни з боку РФ. І Україна гідно бореться із країною-агресором, у тому числі правовими методами. Про них особливо важливо знати кожному, хто хоче надійно захистити свої права та законні інтереси в інформаційному середовищі.

Перш, ніж почати розгляд правових аспектів захисту від інформаційної війни, важливо досконально вивчити основний понятійний апарат даної проблеми. У широкому сенсі, як зазначає Б.С. Льюїс, інформаційна війна (від англ. *information war*) є боротьбою за інформаційний та комунікаційний процеси, це протистояння, яке почалося відразу ж, як з'явилися людське спілкування та конфлікти. У вужчому сенсі, на думку дослідника, йдеться про великомасштабне застосування руйнівної сили проти різних інформаційних систем і активів, а також комп'ютерів і комп'ютерних мереж, задіяних у функціонуванні основних критичних інфраструктур, яких він нарахував чотири – зв'язок, фінансова, транспортна і безпосередньо електросистема. Б.С. Льюїс зазначає, що навіть щодо менш серйозних об'єктів належний рівень захисту від комп'ютерного вторгнення важливий для забезпечення національної безпеки держави [2].

Інститут енциклопедичних досліджень НАН України так визначає вказаний термін: це вплив на жителів іншої держави як у мирний, так і у воєнний час шляхом поширення певних відомостей, а також захист власних громадян від такого впливу [3].

Щодо нормативно-правових джерел, то одним із перших визначення інформаційної війни надав раніше чинний український Стратегічний оборонний бюлетень № 771 у 2012 р., назвавши її формою протистояння між різними суб'єктами за допомогою інформаційного впливу на мешканців країни із використанням ЗМІ, комп'ютерних мереж та подібного. І все це робиться для того, щоб сформувати особливу думку у соціуму, підірвати моральний дух його в цілому та окремих його інститутів зокрема [4].

Зазначимо, що в науці використовуються два терміни як синоніми – інформаційна війна (від англ. *information war*) та інформаційне протиборство (боротьба) (від англ. *information warfare*). Як зазначає Ескалера-Рейєс Дж., другий концепт найбільш популярний у РФ, де під ним розуміють «суперництво соціальних систем у інформаційно-психологічній сфері щодо впливу на ті чи інші сфери соціальних відносин та встановлення контролю над джерелами стра-

тегічних ресурсів, у результаті якого одні учасники суперництва набувають переваги, необхідні їм для подальшого розвитку, а інші їх втрачають» [5].

З урахуванням вищевикладеного, можемо зробити висновок про те, що метою інформаційної війни (далі – ІВ) є значне послаблення як матеріальних, так і моральних ресурсів противника, а разом з тим – і посилення власних. При цьому головним завданням ІВ ми вважаємо маніпулювання масами, їхньою свідомістю. Зазначене сприяє «вкладенню» у свідомість як суспільства, так і окремих індивідів зловмисних, спотворених, вигідних протиборчій стороні поглядів і думок. Зазначимо, що при досягненні вказаного завдання, агресор отримує можливість: сіяти страх серед населення свого супротивника, розвивати у ньому панічні настрої; нести дезінформацію у маси, дезорієнтуючи супротивника; послабити дух іншого народу, зламати його засади та звичаї; змусити владу країни-жертви вдатися до небажаних для нього поступок.

Також у зв'язку із цим зазначимо думку У. Коруц, згідно з якою метою інформаційної кампанії є переконання і українського народу, і всього світу в цілому, в тому, що в Україні чинний режим або недемократичний, або корумпований, або авторитарний. Відповідно, агресор хоче показати, що наша держава перебуває під владою, яка потребує негайного повалення. Саме тому останні майже десять років РФ веде проти нас особливо агресивну інформаційну війну, яка, проте, не дала бажаний ворогом результат у вигляді формування достатнього пропагандистського грунту для виправдання військової агресії. У. Коруц упевнена, що така форма інформаційного протистояння може і має бути кваліфікована як злочин проти порядку, встановленого урядом, а також як очевидний заклик до насильницької зміни політичного режиму [6, с. 335].

На перший погляд, інформаційна війна не результує у реальні жертви, але це не так. Це вид дуже небезпечної зброї, яка «вбиває» державний механізм, а цим таке, відповідно, може призвести до людських жертв.

Як зазначає Р.В. Пилипчук, об'єктами інформаційного протистояння зазвичай стають саме інформаційний простір, комп'ютерні мережі, різні інфоресурси, системи зв'язку та управління тощо. Він називає зразком класичної ІВ холодну війну 1946-1991 рр. між Радянським Союзом та Сполученими Штатами. При цьому вказується на те, що чим більше сучасний соціум «інформатизований», чим більше він залежить від інформації, даних та засобів їх доставки, тим більше він уразливий у разі розвитку інформаційної війни [3].

Види (форми) інформаційної війни (протиборства), згідно з М. Лібіцьки, бувають такими: бойові дії, коли має місце управління військами; розвідувальні дії; психологічна війна; інформаційно-економічна війна; радіоелектронне протиборство; хакерська війна; кібернетична війна [7, с. 1045-1046].

Наразі також відомі такі форми ІВ як мережева війна, семантична війна та ідеологічна диверсія. Але, незалежно від виду, в інформаційній війні завжди як зброя виступає безпосереднє використання інформації.

Найчастіше методи ведення ІВ включають збір тактичних відомостей, ведення пропаганди, деморалізацію противника шляхом поширення дезінформації серед його населення, спроби не дати противнику здійснити збір необхідних даних, або спотворення такої інформації і подібне. Нерідко, особливо у часи засилля інформаційних технологій, інформаційне протистояння ведеться комплексно із кібернетичною і психологічною війнами.

Так, кібервійна – це протистояння безпосередньо у кіберпросторі, наприклад, в Інтернеті. Сюди відносять і DDoS-атаки, про які знає практично кожен українець через агресію проти нас Росії. Кібербезпека та підтримка її на належному рівні в державі – це також одна з «цеглин», на яких стоїть безпека інформаційна. Як зазначає В.В. Філінович, кібербезпека передбачає здійснення дій, які спрямовані на управління ризиками в кіберпросторі, і відповідна активність є функцією як окремих організацій, так і цілих урядів, а її метою є забезпечення конфіденційності, правдивості та доступності даних та інших інформаційних активів у кібер-

нетичному просторі [8, с. 39]. Психологічна війна – це психологічний вплив як на сили, так і на жителів країни-жертви, метою чого є їхня деморалізація.

Розібравшись із основними поняттями та категоріями, перейдемо до аналізу правових засад протидії проявам інформаційної війни. Так, для України, на нашу думку, особливого значення набув ухвалений Єврокомісією у квітні 2016 року документ під назвою «Спільні принципи протидії гібридним загрозам – відповідь Європейського Союзу» (англ. *Joint Framework on countering hybrid threats a European Union response*). Відповідно до нього, держави-члени повинні зайнятися розробкою та впровадженням узгоджених механізмів реалізації стратегічних комунікацій для протидії дезінформації, так само як і для публічного викриття гібридних загроз. Там же наголошується на важливості високоякісного захисту об'єктів критичної інфраструктури, адже гібридні атаки можуть мати результатом відчутні економічні та соціальні порушення. Зазначимо, що у 2017 році українські об'єкти критичної інфраструктури сильно постраждали у зв'язку із засиллям комп'ютерного вірусу *Petya*. Також Joint Framework наголошує на необхідності тісної взаємодії країн ЄС з НАТО щодо стратегічних комунікацій, останні, у свою чергу, повинні включати використання соціальних медіа та традиційні засоби масової комунікації. Окремо вказується на можливість провокаційних дій з боку агресорів у вигляді поширення дезінформації з метою радикалізації окремих осіб та дестабілізації суспільства в цілому. Ще документ наказує, крім іншого, службам зовнішніх зв'язків ЄС забезпечити цілеспрямовану комунікацію для реагування на дезінформацію [9].

Наступним не менш важливим актом стала ухвалена Європейським Парламентом у листопаді того ж року Резолюція «Стратегічні комунікації Європейського Союзу як протидія пропаганді третіх сторін» (англ. *EU strategic communication to counteract propaganda against it by third parties*). Документ включає преамбулу і чотири розділи з 59 пунктів. У ньому сказано не лише про стратегічні комунікації Євросоюзу щодо протидії пропаганді, а й про необхідність викривати російську дезінформацію та пропаганду. Також у п. 2 документа наголошується, що інформаційна війна – це не лише зовнішній, а й внутрішній аспект Європейського Союзу. Пункт 3 відносить дезінформацію та пропаганду до елементів гібридної війни. Пп. 7-14 присвячені інформаційному впливу РФ. Дуже цікавим, на нашу думку, є п. 35, який зазначає, що «розпалювання ненависті, насильства або війни не може «ховатися» за ширмою свободи вираження поглядів». Важливим нюансом цієї Резолюції слід вважати вказівку на те, що гібридна війна націлена на послаблення стратегічної єдності Європейського Союзу та його північноамериканських партнерів, так само як і на порушення процесу прийняття рішень відповідними органами, а також дискредитацію інститутів ЄС та трансатлантичного партнерства. Документом Європарламент визнав і агресивне використання російською владою великого набору інструментів і методів для атаки на демократичні цінності, а з ним – і розколу Європи, а також для формування враження про розбіжності між східними країнами Союзу [10]. В Україні цю резолюцію також називають «ухвалою про протидію російській пропаганді».

Що стосується національних нормативно-правових актів, то в Україні є низка документів щодо правових аспектів інформації та інформаційного простору, серед них особливого значення набули закони № 2657-XII «Про інформацію» (від 02.10.1992), № 74/95-ВР «Про інформаційні агентства» (від 28.02.1995), № 2782-XII «Про друковані засоби масової інформації (пресу) в Україні» (від 16.11.1992), № 75/98-ВР «Про Концепцію Національної програми інформатизації (від 04.02.2019) та інші. Але особливо важливими для наших цілей є нормативно-правові акти з питань забезпечення інформаційної безпеки як ключового аспекту у запобіганні та протидії проявам інформаційного протистояння. Так, своїм указом № 47 від 25 лютого 2017 року тодішній український президент надав чинності Рішенню Ради Національної Безпеки та оборони (далі – РНБО) про Доктрину інформаційної безпеки України. Документ визначив повноваження відповідних органів із захисту суспільних інтересів в інфор-

маційній сфері та безпосередньо національному інформаційному просторі. Доктрина уточнила основи формування та реалізації державної інформаційної політики, в якій перше місце відведено протидії деструктивному інформаційному впливу РФ в умовах гібридної війни, що нею проводиться проти нашої держави. Документ також розмежував питання урядових та стратегічних комунікацій, що допомогло зосередитися саме на питаннях сектору безпеки та оборони [11].

Зазначимо, що Доктрина потребує доопрацювань та уточнень. Так, вимагає уточнення взаємозв'язок понять «інформаційна безпека» та «кібербезпека», оскільки кібернетичний простір – це елемент інформаційного простору держави. Видалення відповідних прогалин допоможе зробити ефективнішими заходи інформаційного протиборства з боку України. Також важливо врегулювати особливості залучення громадянського суспільства до активностей із забезпечення інформаційної безпеки.

Указом Президента № 685 у грудні 2021 року було запроваджено рішення РНБО «Про Стратегію інформаційної безпеки». Документ визначає актуальні виклики та загрози українській національній безпеці саме в інформаційному середовищі, а також завдання та цілі щодо протидії зазначеному. Окремо Стратегія торкається питання захисту прав на інформацію та захисту персональних даних. Саме посилення можливостей забезпечення інформаційної безпеки України та її інформаційного простору є основною метою документа, а з ними – захист державного суверенітету, територіальної цілісності країни, демократичного конституційного ладу, а також забезпечення прав та свобод українців [12].

Таким чином, наша держава має правові засоби протидії інформаційному протистоянню. Не менш важливо для зазначених цілей проводити просвітницьку діяльність серед населення, привчати його «фільтрувати» новини, що надходять, відрізняти явно дезінформаційні «вкидання» від реальних даних. Для цього важливо запроваджувати серед українців засади інформаційної гігієни.

Висновки. Отже, сьогодні Україна активно бореться з агресією Російської Федерації у вигляді гібридної війни. Не лише військові активи потрапляють «під атаку», а й інформаційний простір та соціальні взаємодії у ньому. Сьогодні більшості з нас уже зрозуміло, що інформаційна кампанія країни-агресора, що проводиться на оперативному рівні, здатна суттєво вплинути та створити значні перешкоди у прийнятті важливих для нашої країни рішень, а таке може дати противнику можливість досягати своїх зловмисних та безчесних цілей. Наш ворог веде активну шпигунську діяльність, намагається перехоплювати важливі дані та несанкціоновано входити в наші інформаційні ресурси з подальшою їхньою фальсифікацією. Не менш активно країна-агресор представляє в українських інформаційних каналах дезінформацію, веде активну пропаганду, щоб вплинути на думку українських громадян про роботу державних органів, підірвати авторитет останніх та дискредитувати чинну владу.

Всі ці та подібні дії здатні завдати величезних збитків життєво важливим інтересам України в економічній, політичній, оборонній та інших сферах, як і підірвати авторитет нашої держави на міжнародному рівні. Росія має сьогодні передові можливості розвідки для ведення інформаційної та кібервійни та використала їх у Сирії та на Донбасі, а також застосовує їх у своєму нинішньому вторгненні до нашої держави.

Але наша держава готова і вже протидіє нечесним діям противника. Проблема забезпечення інформаційної безпеки як важливого інструменту боротьби з інформаційною війною сьогодні актуальна як ніколи. Влада використовує стандартні загальноприйняті методи інформаційної діяльності, окрему роль у чому відіграє саме правове регулювання у сфері державної інформаційної діяльності держави. При цьому головним завданням правового забезпечення інформаційної безпеки стало перетворення змісту національної інформаційної політики в якісне інформаційне законодавство.

Діючі в державі механізми правового захисту та забезпечення інформаційної безпеки активно застосовуються, але все ж таки вимагають удос-

коналення. Важливо також опрацювати та впровадити дієву стратегію-план поведінки в інформаційній війні, до такої діяльності варто залучити досвідчених політологів та представників академічних кіл у сфері інформаційного права. Також необхідно всіма доступними засобами зміцнювати та підвищувати імідж України на світовій арені.

Сьогодні гібридна війна, а з нею й інформаційне протистояння між Україною та Росією продовжуються, відповідно, цю наукову статтю буде надалі доповнено з урахуванням результатів проведення аналізу світової практики боротьби з інформаційними війнами.

Література

1. Sopilko I.M., Iurynets J.L. et al (2020). Problems of implementation of state policy in the field of information security of Ukraine. Ottawa, Canada: Accent Graphics Communications & Publishing.

2. Lewis B.C. Information Warfare. Intelligence Resource Program. URL: https://irp.fas.org/eprint/snyder/infowarfare.htm (дата звернення: 10.03.2022).

3. Пилипчук Р.В. Інформаційна війна. Енциклопедія Сучасної України: електронна версія / гол. редкол.: І.М. Дзюба, А.І. Жуковський, М.Г. Железняк та ін.; НАН України, НТШ. Київ: Інститут енциклопедичних досліджень НАН України, 2011. URL: https://esu.com.ua/search_articles.php?id=12460 (дата звернення: 13.03.2022).

4. Стратегічний оборонний бюлетень України: схвалений Указом Президента України від 29 груд. 2012 р. № 771/2012. URL: https://zakon.rada.gov.ua/laws/show/771/2012#n16 (дата звернення: 12.03.2022).

5. Escalera-Reyes J. Place Attachment, Feeling of Belonging and Collective Identity in Socio-Ecological Systems: Study Case of Pegalajar (Andalusia-Spain). Sustainability 2020, 12, 3388. URL: https://doi.org/10.3390/su12083388.

6. Коруц У. Інформаційна війна як інструмент пропаганди війни: правові підстави протидії. *Entrepreneurship, Economy and Law*. 2020. № 8. С. 334–339. URL: https://doi.org/10.32849/2663-5313/2020.8.55 (дата звернення: 12.03.2022).

7. Damjanovic D. Types of information warfare and examples of malicious programs of information warfare. *Vojnotehnicki glasnik.* 2017. Vol. 65. No. 4. P. 1044–1059. URL: https://doi. org/10.5937/vojtehg65-13590 (date of access: 12.03.2022).

8. Filinovych V. Cybersecurity and threats to the aviation sector: legal aspect. Scientific Works of National Aviation University. Series: Law Journal «Air and Space Law». 2021. № 3(60). P. 38–44. DOI: https://doi.org/10.18372/2307-9061.60.15950.

9. Joint Framework on countering hybrid threats a European Union response. URL: http://bit.ly/2t0ywSh (дата звернення: 14.03.2022).

10. European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties. URL: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0441+0+DOC+XML+V0//EN (дата звернення: 14.03.2022).

11. Про Доктрину інформаційної безпеки України: Рішення РНБО від 29 груд. 2016 р. № 0016525-16. URL: https://zakon.rada.gov.ua/laws/show/ n0016525-16#n2 (дата звернення: 14.03.2022).

12. Про рішення Ради національної безпеки і оборони України від 15 жовт. 2021 р. «Про Стратегію інформаційної безпеки»: Указ Президента України; Стратегія від 28 груд. 2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 14.03.2022).

References

1. Sopilko I.M., Iurynets J.L. et al (2020). Problems of implementation of state policy in the field of information security of Ukraine. Ottawa, Canada: Accent Graphics Communications & Publishing.

2. Lewis B.C. Information Warfare. Intelligence Resource Program. URL: https://irp.fas.org/eprint/snyder/infowarfare.htm (data zvernennja: 10.03.2022).

3. Pylypchuk R.V. Informacijna vijna. Encyklopedija Suchasnoi’ Ukrai’ny: elektronna versi-

ja / gol. redkol.: I.M. Dzjuba, A.I. Zhukovs'kyj, M.G. Zheleznjak ta in.; NAN Ukrai'ny, NTSh. Kyi'v: Instytut encyklopedychnyh doslidzhen' NAN Ukrai'ny, 2011. URL: https://esu.com.ua/search_articles.php?id=12460 (data zvernennja: 13.03.2022).

4. Strategichnyj oboronnyj bjuleten' Ukrai'ny: shvalenyj Ukazom Prezydenta Ukrai'ny vid 29 grud. 2012 r. № 771/2012. URL: https://zakon.rada.gov.ua/laws/show/771/2012#n16 (data zvernennja: 12.03.2022).

5. Escalera-Reyes J. Place Attachment, Feeling of Belonging and Collective Identity in Socio-Ecological Systems: Study Case of Pegalajar (Andalusia-Spain). Sustainability 2020, 12, 3388. URL: https://doi.org/10.3390/su12083388.

6. Koruc U. Informacijna vijna jak instrument propagandy vijny: pravovi pidstavy protydii'. *Entrepreneurship, Economy and Law.* 2020. № 8. S. 334–339. URL: https://doi.org/10.32849/2663-5313/2020.8.55 (data zvernennja: 12.03.2022).

7. Damjanovic D. Types of information warfare and examples of malicious programs of information warfare. *Vojnotehnicki glasnik.* 2017. Vol. 65. No. 4. P. 1044–1059. URL: https://doi.org/10.5937/vojtehg65-13590 (date of access: 12.03.2022).

8. Filinovych V. Cybersecurity and threats to the aviation sector: legal aspect. *Scientific Works of National Aviation University. Series: Law Journal «Air and Space Law».* 2021. № 3(60). P. 38–44. DOI: https://doi.org/10.18372/2307-9061.60.15950.

9. Joint Framework on countering hybrid threats a European Union response. URL: http://bit.ly/2t0ywSh (data zvernennja: 14.03.2022).

10. European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties. URL: http://www.europarl.europa.eu/sides/ getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0441+0+DOC+XML+V0//EN (data zvernennja: 14.03.2022).

11. Pro Doktrynu informacijnoi' bezpeky Ukrai'ny: Rishennja RNBO vid 29 grud. 2016 r. № 0016525-16. URL: https://zakon.rada.gov.ua/laws/show/n0016525-16#n2 (data zvernennja: 14.03.2022).

12. Pro rishennja Rady nacional'noi' bezpeky i oborony Ukrai'ny vid 15 zhovt. 2021 r. «Pro Strategiju informacijnoi' bezpeky»: Ukaz Prezydenta Ukrai'ny; Strategija vid 28 grud. 2021 r. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/ 685/2021#Text (data zvernennja: 14.03.2022).

Iryna Sopilko

INFORMATION WAR AGAINST UKRAINE AND LEGAL MEANS TO COUNTER ILLEGAL ACTIONS

National Aviation University
Liubomyra Huzara Avenue, 1, 03680, Kyiv, Ukraine
E-mail: sopilko_i@ukr.net

As you know, Ukraine has long been drawn into a hybrid war, an integral element of which is the information war. In the context of the latter, cybernetic warfare also stands out. In general, attempts to influence the consciousness of individuals and even entire social groups with the help of information have been known since the emergence of the human race, as evidenced by founded traditions and stereotypes. At this stage of human development, when the use of information networks has become an integral element of daily interaction, it is information weapons that have become the main tool and driving force among the world's power actors.

For more than eight years, the Russian Federation has waged hybrid war against Ukraine. In February 2022, Russia began ruthlessly killing Ukrainian civilians, bombing non-military facilities, and in other ways violating the norms and foundations of international law in general and international humanitarian law in particular. At the same time, with no less fury, the aggressor country is trying to exert an informational influence both on the citizens of Ukraine by throwing in fakes and propaganda, and on its people, placing them in an information vacuum. There are attempts by the adversary to gain control over the means of transmitting information, especially concerning the World Wide Web. The purpose of such actions is to force people to think in the way the enemy wants, to impose his goals and principles on the victims.

Therefore, it is important to know what an information war is, no less valuable for every Ukrainian will be an understanding of how to counteract the aggressive actions of the enemy in the information space. A detailed acquaintance with the legal methods of countering illegal activity during the information war will help Ukrainians protect their information rights and interests. This is what will be discussed in this scientific study.

Purpose of the paper: *to study the features and essence of the information war and give recommendations on the legal regulation of relevant issues in Ukraine.* ***Research methods:*** *this scientific article was written by the author using generally recognized methods of scientific knowledge, namely, analytical, formal, comparative-legal, system-structural, and others.* ***Results:*** *the concept, essence, characteristics of information warfare and related categories are analyzed, the problems of ensuring counteraction to malicious acts in this area are indicated, recommendations are provided for overcoming such problems by improving the current legislation, including through the experience of other countries and harmonizing the current regulatory framework with EU standards.* ***Discussion:*** *the dialogue in the scientific study is about the peculiarities of the legal regulation of the threats and risks faced by Ukraine during the hybrid and forthright information war waged against it.*

Key words: *information war; information security; cyber warfare; hybrid warfare; state security.*

Стаття надійшла до редакції 22.08.2022