

ДЕСТРУКТИВНИЙ ІНФОРМАЦІЙНИЙ ВПЛИВ ЯК ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ ВІЙНИ

«Сутністю будь-якої війни – є обман!»

Сунь-Цзи

Анотація. У статті констатовано, що з моменту проголошення України незалежною державою розпочався стрімкий перехід від тоталітаризму до демократії. Однак, окрім позитивних змін є й певні негативні моменти, які можуть нести загрозу національному суверенітету на фоні розв'язаної російською федерацією війни. Сприяла цьому й підтримка військової агресії окремими громадянами, що обумовлено цілеспрямованим впливом на їх (насамперед молоді) свідомість і підсвідомість та формування антигромадської позиції (недовіри до чинної влади, правоохоронних і спеціальних органів, Збройних сил України тощо), а також спонукання до вчинення актів непокори чи інших протиправних дій. Вказане відбувається, у тому числі й у наслідок здійснення системного деструктивного впливу.

Зважаючи на викладене, **метою статті** є аналіз поняття «деструктив», та окреслення організаційних і правових методів протидії вказаному негативному явищу (у тому числі й у мережі Інтернет).

Констатовано увагу на тому, що організована співробітниками спеціальних служб РФ системна та комплексна дезінформація на сьогодні є актуальною загрозою державному суверенітету і територіальній цілісності України. Зазначене вимагає удосконалення: правової регламентації поширення інформації, порядку обмеження доступу до неї у випадках фейковості; методик і правових підстав притягнення до відповідальності суб'єктів, причетних до розповсюдження дезінформації.

Стверджується, що деструктивний інформаційний вплив, який супроводжує зовнішню збройну агресію і реалізується у внутрішньому інформаційному просторі України, має на меті зміцнити антиукраїнські позиції шляхом цілеспрямованого тиску на державні інституції, поляризації суспільства та підміни традиційних національних цінностей. У контексті протидії такому впливу поширюється дискусія щодо: меж державного втручання в інформаційну сферу, оскільки демократія може існувати лише за наявності сильних і незалежних засобів масової інформації, гарантування кожному права на свободу слова і вираження своїх поглядів; дотримання демократичних принципів у контексті протистояння зброї так званого «масового інформаційного ураження».

У заключній частині дослідження, за результатами вивчення експертних напрацювань, визначено ряд заходів, імплементація яких дозволить підвищити ефективність протидії використанню мережі Інтернет з метою здійснення деструктивних інформаційних впливів.

Ключові слова: деструктивний інформаційний вплив, інформаційна війна, мережа Інтернет, протидія деструктивному інформаційному впливу.

Постановка проблеми. Суперництво, що розгортається за володіння інформаційним

ресурсом в широкоспектральному світовому просторі, стає ареною запеклої геополітичної конкуренції, дієвим ін-

струментом впливу на міжнародне співтовариство, громадську думку та національну безпеку держав.

Аналіз процесів у сфері забезпечення національної безпеки свідчить, що поряд з відкритими військовими операціями, для досягнення стратегічного і тактичного успіху агресор (противник) поширює тенденційні відомості з використанням електронних, соціальних та інших мереж. Ці мережі можуть одночасно використовуватись для прихованого політичного, економічного, психологічного примусу та викривлення сприйняття реальності громадянами.

У процесі реалізації деструктивного інформаційного впливу створюються передумови порушення сталого функціонування інститутів держави, руйнації психіки широких кіл суспільства.

У процесі підготовки спеціальних інформаційних акцій та операцій, представники спеціальних служб російської федерації використовують фахові знання теоретиків і навички практиків у галузях політики, економіки, військової сфери тощо. Для цього застосовуються передові технології та психологічні прийоми, які у поєднанні із специфічними можливостями сил безпеки і оборони країни-агресора можуть викликати значний суспільний резонанс.

Реалізація таких акцій та операцій може у короткостроковій перспективі призвести до дестабілізації суспільно-політичної ситуації в окремому регіоні та Україні у цілому, дискредитації країни на міжнародній арені, виникнення осередків соціальної напруги, військових поразок локального і ширшого масштабу. У довгостроковій перспективі – до поступової зміни світогляду і переконань громадян, деформації національної ідеї, втрати національної ідентифікації, у тому числі й шляхом підміни реальних сталих спогадів на необ'єктивні та недостовірні (фейкові). Окремо слід відмітити, що у короткостроковій та довгостроковій перспективі одночасно можуть вирішуватися питання зміни полі-

тичної, економічної, військової, наукової та інших еліт.

Організована співробітниками спеціальних служб РФ системна та комплексна дезінформація на сьогодні є актуальною загрозою державному суверенітету і територіальній цілісності України. Зазначене вимагає удосконалення: правової регламентації поширення інформації, порядку обмеження доступу до неї у випадках фейковості; методик і правових підстав притягнення до відповідальності суб'єктів, причетних до розповсюдження дезінформації.

Україна стикнулася з низкою викликів і загроз, спричинених деструктивним інформаційним впливом. Зокрема, з ускладненням критичного сприйняття інформаційного потоку населенням, зростанням недовіри до офіційних новин і медіа, зниженням довіри до демократичних інститутів, правлячої еліти, Збройних Сил України, спеціальних і правоохоронних органів тощо.

Деструктивний інформаційний вплив, який супроводжує зовнішню збройну агресію і реалізується у внутрішньому інформаційному просторі України, має на меті зміцнити антиукраїнські позиції шляхом цілеспрямованого тиску на державні інституції, поляризації суспільства та підміни традиційних національних цінностей. У контексті протидії такому впливу поширюється дискусія щодо: меж державного втручання в інформаційну сферу, оскільки демократія може існувати лише за наявності сильних і незалежних засобів масової інформації, гарантування кожному права на свободу слова і вираження своїх поглядів; дотримання демократичних принципів у контексті протистояння зброї так званого «масового інформаційного ураження».

Аналіз останніх наукових досліджень та публікацій. Питання протидії деструктивним інформаційним впливам, системній дезінформації обговорюється на національному і світовому рівнях із залученням визнаних і авторитетних

представників міжнародних інституцій, фахівців та експертів високого рівня. Такий підхід є досить корисним, у першу чергу, для країн так званої «молодої» демократії.

Розуміючи наслідки деструктивних інформаційних впливів, все більше науковців різних країн світу звертають увагу на вивчення зазначеного питання. Назвемо лише деяких з них, абсолютно не применшуючи досягнення та значущість інших науковців і дослідників. Зокрема це: А. Благодарний, М. Галамба, В. Горбулін, О. Довгань, В. Домарєв, І. Доронін, Л. Кампанцева, В. Крутов, І. Литвиненко, В. Ліпкан, А. Марущак, В. Остроухов, С. Расторгуєв, Д. Рісман, Т. Рон, В. Петрик, Г. Перепелиця, В. Пилипчук, М. Погорецький, В. Полевий, Г. Почепцов, Д. Сергєєва, Т. Ткачук, З. Топорецька, А. Черняк та інші. Окремі питання окресленої проблематики розглядалися й нами у відповідних наукових працях^{1,2,3,4,5}.

З огляду на викладене, виникає необхідність у комплексному узагальненні раніше напрацьованих теоретичних розробок з досліджуваної проблематики та розбудови на їх основі дієвої системи протидії деструктивному інформаційному впливу.

Метою статті є критичний аналіз підходів до сутності «деструктиву», об'єктів та завдань деструктивного інформаційного впливу, який реалізується і в ході інформаційної війни (у тому чис-

лі й у мережі Інтернет). Окреслена тематика є мультидисципліною і вимагає ґрунтовного теоретичного опрацювання науково-прикладних здобутків різних галузей: права, психології, кібербезпеки, інформаційної безпеки тощо.

Виклад матеріалу дослідження та його основні результати. Зважаючи на швидкий процес розвитку інформаційно-комунікаційних технологій, провідні науковці зосереджуються на дослідженні специфіки використання інформації у життєво важливих сферах суспільного життя.

Інформація є однією з основних складових взаємодії особи та держави. В умовах збройного протистояння вона стає важливим інструментом ведення «гібридної війни», який дозволяє формувати громадську думку, виступає каталізатором протестного потенціалу. Тому розуміння інформації як доктринальної категорії має фундаментальне значення для розкриття теми нашого дослідження⁶.

Багатоспектральність інформаційної сфери на сьогодні неможливо уявити без інформаційного впливу, у тому числі деструктивного характеру. Його реалізація протиборчою стороною зумовлена необхідністю досягнення визначених цілей в короткостроковій або довгостроковій перспективах.

З моменту проголошення України незалежною державою розпочався стрімкий перехід від тоталітаризму до демократії. Однак, на фоні позитивних змін

¹ M Pohoretskyi, A Cherniak, D Serhieieva, R Chernysh та Z Toporetska, Detection and proof of cybercrime (2022) 11(53) *Amazonia Investiga* 259–269 <<https://doi.org/10.34069/AI/2022.53.05.26>>.

² Р Черниш, М Ігнатюк, О Заріцький, Протидія деструктивному інформаційному впливу в Україні: правові та організаційні аспекти (2022) 1 *Юридичний науковий електронний журнал* <<http://www.lsej.org.ua/index.php/arkhiv-nomeriv?id=146>> дата звернення 04.12.2023.

³ Р Черниш, Організаційні та правові методи протидії маніпулюванню свідомістю громадян у соціальних мережах (2020) 3–4 *Вісник кримінального судочинства* 168–177 <<https://doi.org/10.17721/2413–5372.2020.3–4/168–177>>.

⁴ Р Черниш, Фейк, як один із інструментів негативного впливу на національну безпеку України в умовах ведення гібридної війни (2019) 2 *Часопис київського університету права* 109–114 <http://kul.kiev.ua/doc/chasopys2019/CHAS_19_2.pdf> дата звернення 05.12.2023.

⁵ Р Черниш Соціальні мережі, як один із інструментів накопичення та протиправного використання персональних даних громадян (2017) 136 *Проблеми законності* 205–214.

⁶ Докладно про визначення поняття інформації та використання її в діяльності правоохоронних органів та спецслужб див: М А Погорецький, Оперативно-розшукова інформація: до визначення поняття (2007) 36 *Вісник Харківського нац. ун-ту внутр. справ* 13–19; М А Погорецький, Оперативно-розшукова інформація. *Міжнародна поліцейська енциклопедія*: у 10 т. Т. VI: Оперативно-розшукова діяльність поліції (міліції) / відп. ред. В В Коваленко, Є В Моїсєєв, В Я Тацій, Ю С Шемшученко (Київ, Атіка, 2010) 570–572.

виникли суттєві негативні моменти, що створюють передумови до загроз національному суверенітету, територіальній цілісності України та іншим складовим національної безпеки. Каталізатором цих проявів стала зовнішня збройна агресія.

Підтримка агресії окремими громадянами, спонукання до вчинення актів непокори чи інших протиправних дій є результатом цілеспрямованого деструктивного впливу противника на їх свідомість і підсвідомість. При цьому українці, маючи вільний доступ до значних інформаційних ресурсів, через деяку інертність і недостатність знань щодо застосування інформаційних технологій, не відразу почали розуміти, що проти них ведеться інформаційна війна з використанням деструктивного інформаційного впливу, критично осмислювати потік отримуваної інформації.

До категорії «деструктив» та вивчення її проявів вперше комплексно підійшов німецький психолог і психоаналітик Е. Фромм, який ввів у науковий обіг термін «деструктивність» як специфічну злостісну форму агресії та руйнування. У своїх дослідженнях він стверджував, що «деструктивність не є вродженим людським інстинктом, це властивість, яка народжена людиною»¹. Погоджуючись із думкою Е. Фромма, одночасно слід зазначити, що деструктивність це не лише властивість, народжена людиною, а й властивість, яка нею використовується на особистісному та суспільному рівнях з метою інформаційного впливу.

Об'єктами та сферами деструктивного інформаційного впливу традиційно є: ідеологічно-психологічне середовище суспільства; ресурси, що розкривають духовні, культурні, історичні та інші цінності, надбання держави і нації в різних сферах; інформаційна інфраструктура; системи формування суспільної свідомості, громадської думки; система розроблення та прийняття політичних рішень; свідомість і поведінка людини².

У процесі реалізації деструктивного інформаційного впливу його об'єктами також стають певна цільова аудиторія, зокрема, психіка представників політичної еліти й населення конфронтуючих держав, система формування та прийняття державно-управлінських рішень у сфері національної безпеки.

До основних завдань деструктивного інформаційного впливу фахівці та експерти відносять: маніпулювання суспільною свідомістю і політичною орієнтацією населення держави; суспільну дестабілізацію; введення населення в оману щодо роботи органів державної влади; провокування соціальних, політичних, національно-етнічних і релігійно-конфесійних сутичок; дискредитацію фактів історичної, національної самобутності народу; зміну системи цінностей, котрі визначають спосіб життя і світогляд людей; створення атмосфери бездуховності; підризу міжнародного авторитету держави; формування передумов для економічної, воєнної чи духовної поразки; підризу морального духу та психологічної стабільності населення, обороноздатності й бойового потенціалу держави.

З урахуванням активізації діяльності спеціальних служб під час збройного протистояння, до сфери деструктивного інформаційного впливу доцільно також віднести діяльність національних спецслужб і правоохоронних органів та нівелювання досягнутих ними результатів.

На сьогодні такий вплив активно застосовується агресором під час інформаційної війни, яка є різновидом бойових дій, зброєю в яких виступають обладнання та методи обробки інформації, що дозволяють цілеспрямовано, швидко і потай впливати на військові й цивільні інформаційні системи з метою підризу політики, економіки, боєздатності, а в остаточному підсумку – інформаційну складову державної безпеки. Погоджуємося із твердженням про те, що поняття

¹ Е. Фромм, Втеча від свободи (Харків, Книжковий Клуб «Клуб Сімейного Дозвілля», 2019) 288.

² В. Петрик, Сутність інформаційної безпеки держави, суспільства та особи (2009) *Юридичний журнал* <<http://www.justinian.com.ua/article.php?id=3222>> дата звернення 05.12.2023.

інформаційної війни є на сьогодні одним із найпопулярніших, зокрема тому, що людство живе у так звану інформаційну епоху¹.

Акції деструктивного інформаційного впливу як складової інформаційної війни можуть націлюватись на широкий спектр суспільних відносин та життєво важливі сфери забезпечення національної безпеки (політику, економіку, військову та оборонну сфери, науку тощо). Поряд з тим, вони можуть реалізовуватися і у форматі вчинення кіберзлочинів².

Вперше термін інформаційна війна застосував у 1920 році британський історик Дж. Фуллер, який проаналізував хід Першої світової війни. Цей термін взяли на озброєння американці. У 1966 році А. Даллес у своїй книзі «Таємна капітуляція» вжив це словосполучення для визначення особливого виду спецоперацій розвідки³. У 1976 році термін «інформаційна війна» використав майбутній радник міністерства оборони та Білого дому за часів президентства Р. Рейгана і Дж. Буша, фізик Т. Рон у звіті «Системи зброї й інформаційна війна». Він зазначив, що інформаційна складова є невід'ємним компонентом американської економіки і може стати вразливою ціллю в мирний чи воєнний час та визначив місце і роль інформаційної складової в процесах нагнітання «холодної війни». У вказаному документі Т. Рон виклав своє бачення концепції інформаційних війн, яка зводиться до ідеї «зниження інформаційного потоку супротивника та, натомість, захисту або вдосконалення свого власного», а також підкреслив, що швидкість реакції в інформаційній війні є вирішальним елементом для перемоги. У цьому сенсі вразливими є всі, без ви-

нятку, країни світу. США також можуть стати об'єктом інформаційної атаки, а їх супротивники – переконати американську громадськість у «своїй правді» шляхом розумного маніпулювання засобами масової інформації⁴.

Погоджуючись з висновком американського дослідника, слід зазначити, що концепцію інформаційних війн, «зниження інформаційного потоку супротивника та, натомість, захист або вдосконалення свого власного», на нашу думку, доцільно доповнити ідеєю переорієнтування інформаційного потоку на союзників противника. При цьому слід враховувати, що такі союзники можуть займати в інформаційному протистоянні активну або пасивну позицію та змінювати її залежно від стану і тенденцій розвитку оперативної обстановки, зокрема при підвищенні або зниженні «градусу» власних інтересів.

Українські дослідники, розглядаючи поняття «інформаційна війна», ще не дійшли згоди із формування єдиного підходу до його розуміння. Це пояснюється певним «застарінням» тих чи інших поглядів на генезу інформаційної війни, яка стала динамічним явищем в умовах розвитку інформаційних технологій.

М. Лібікі у своїй книзі «Що таке інформаційна війна?», яка вважається у наукових колах класичною, визначив сім форм інформаційної війни, зосередив основну увагу на розкритті їх прояву залежно від напрямів ведення війни, зокрема:

1. Командування та управління (command-and-control – C2W) – військова стратегія, яка реалізує інформаційну війну на полі бою та об'єднує фізичне знищення.

¹ Я Малик, Інформаційна війна і Україна (2015) 15 *Науковий вісник «ДЕМОКРАТИЧНЕ ВРЯДУВАННЯ»* 27.

² М Погорецький, В Шеломенцев, Поняття кіберпростору як середовища вчинення злочинів (2009) 2 *Інформаційна безпека людини, суспільства, держави* 77–81; М Погорецький, В Шеломенцев, Кіберзлочини: до визначення поняття (2012) 8 *Вісник прокуратури* 89–96; М Погорецький, В Шеломенцев, Правове забезпечення боротьби з кіберзлочинами в Україні: проблемні питання. (2011) 8 (122) *Вісник прокуратури* 30–38.

³ A Dulles, The Secret Surrender. Harper & Row (1966) <https://books.google.de/books/about/The_Secret_Surrender.html?id=b3kNAAAAIAAJ&redir_esc=y> дата звернення 06.12.2023.

⁴ T Ron, Weapon Systems and Information War (Boeing Aerospace Co. Seattle WA, 1976) <https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf> дата звернення 07.12.2023.

2. Військова розвідка (intelligence-based warfare IBW) – збір важливої та захист власної інформації.

3. Електронна війна (electronic warfare EW) – спрямована проти засобів електронних комунікацій: радіозв'язку, телевізійних мереж, комп'ютерних мереж, радарів.

4. Психологічна війна (psychological warfare PSYW) – охоплює використання інформації проти людського розуму.

5. Хакерська війна (hacker warfare) – диверсійні дії та атаки проти ворога шляхом створення спеціальних програм, атак на комп'ютерні мережі.

6. Економічна інформаційна війна (economic information warfare EIW), яка має дві форми: інформаційна блокада, яка полягає в обмеженні однією державою доступу до інформації іншої; і інформаційний.

7. Кібервійна – здійснюється у формі інформаційного тероризму, семантичних атак, симульованих війн, війн Гібсона (ведення війни у віртуальному просторі за допомогою інтелекту¹).

Погоджуючись із автором, окремо відмітимо, що при будь-якій із форм реалізації інформаційної війни може здійснюватися деструктивний інформаційний вплив на свідомість.

У той же час, на нашу думку, М. Лібікі не акцентує увагу на визначенні ролі спеціальних служб (розвідки та контррозвідки) у реалізації форм інформаційної війни. На сьогодні стан оперативної обстановки на глобальному і регіональному рівнях та тенденції її розвитку дають підстави для визначення ще однієї, восьмої форми такої війни – проведення спецслужбами спеціальних інформаційних операцій. Ці операції передбачають втаємничення їх організації та здійснення, комплексне задіяння наявних сил і засобів.

Деструктивний інформаційний вплив, за висновками науковців, може

здійснюватись у ході інформаційної війни або ще до її початку. Зокрема, як зазначає О. Свідерська, ще до повномасштабного вторгнення агресора відбувалося «розгойдування» емоційно-психологічного стану українців. Україна постійно піддавалася кібер-атакам з боку противника: численні фейки, пропаганда, дезінформація, інформаційні викиди, атаки на офіційні сторінки різноманітних державних відомств, псевдозамінування вокзалів, шкіл і супермаркетів, повідомлення про можливе повномасштабне втручання на територію держави. Це мало ознаки стратегічних інформаційно-психологічних спецоперацій, метою яких було дестабілізувати та дезорієнтувати українське суспільство, посіяти ворожість, паніку та змусити країну піти на поступки агресору².

Деструктивний інформаційний вплив включає у себе суб'єкт і об'єкт. Суб'єктами під час військових дій, у першу чергу, будуть держави, що беруть у них участь. Державні органи зацікавлені у формуванні «правильної» суспільної думки в своїй країні та в інших країнах. Будь-який інформаційний вплив під час збройних зіткнень контролюється державою, оскільки вона має найбільш достовірну інформацію про події на території конфлікту. При цьому необхідно враховувати, що протидіючі сторони не завжди мають достовірну інформацію у зоні конфлікту, оскільки з обох боків вживаються заходи щодо приховування реальних, об'єктивних та актуальних даних, у тому числі шляхом дезінформації ворога.

Об'єктом деструктивного інформаційного впливу є людина, суспільство і держава – ті об'єкти, на захист яких або проти яких він спрямовується.

При цьому, ефективність інформаційних впливів під час ведення інформаційних воєн визначається передусім умінням використовувати саму інфор-

¹ M Libicki, What is information warfare? (Washington, National Defense University Press, 1995) 104 <http://www.dodccrp.org/files/Libicki_What_Is.pdf> дата звернення 08.12.2023.

² О Свідерська, Цифрова пропаганда та ризики інформаційної безпеки у контексті російсько-української війни *Науковий журнал «Політикус»* <<http://politicus.od.ua/>> дата звернення 09.12.2023.

мацію. Складна когнітивна-аксіологічна природа інформації штовхає до пошуку новітніх тактичних та стратегічних прийомів для здійснення інформаційних впливів, які допоможуть досягти бажаних завдань та мети¹.

Об'єктивна реальність сьогодні така, що майже десять років війни на території України, системні економічні турбулентності, об'єми даних, що циркулюють, не завжди дозволяють критично проаналізувати інформацію, якої з кожним днем стає все більше. Саме інформація визначає напрям руху суспільства в цілому. Розвиток демократії, впровадження реформ тощо залежить у тому числі й від того, наскільки в своїй масі громадяни зможуть «фільтрувати» інформацію і дотримуватись «інформаційної гігієни». Інакше, при відсутності у «критичної» маси населення, будь-які позитивні зміни (медичні, освітні, економічні, військові реформи, а також реформи спецслужб і правоохоронних органів) можуть бути досить легко дискредитованими з ініціативи зацікавлених суб'єктів (зовнішній агресор, внутрішні дестабілізуючі сили).

На сьогодні пересічному громадянину досить важко проаналізувати значний масив відкритої інформації, що зумовлено її обсягом, суперечливістю, наявністю фейків та недостатністю офіційних коментарів, а також недовірою до органів державної влади. Зазначене, під дією страху і стресу, які впливають на наше сприйняття інформації, дозволяє у максимально стислі терміни поширювати інформаційні віруси та здійснювати деструктивний інформаційний вплив.

У країнах з «новими демократіями», які не сформувалися до початку цифрової ери, інформація, впливаючи на населення, може змінювати тренди, визначати напрям державної політики та кардинально змінювати відношення до тих чи інших груп всередині суспільства.

Вказана проблема стала більш актуальною з розв'язанням російською федерацією «гібридної війни» щодо України. Так, у Центрі інформаційної безпеки фсб рф до початку війни в Україні нараховувалося понад 800 співробітників, а відділ інформаційної ізоляції, який займається проведенням інформаційних операцій на Донбасі складається із 60 осіб.

Крім виключно інформаційних акцій проти України ведеться ще й кібервійна. За словами спікера Українського кіберальянсу, російськими хакерами керує фсб та адміністрація президента рф. Причому є підтвердження наявності зв'язків російських держорганів з відомими кіберзлочинцями, що відкриває їхнім спецслужбам додаткові можливості².

За висновками профільних фахівців та експертів, розробка дієвих способів протидії деструктивним інформаційним впливам та ефективність їх застосування відстає від потреб правоохоронної практики, що потребує поглиблених наукових досліджень, у тому числі із застосуванням емпіріокритичного методу.

В контексті організації ефективної протидії деструктивному інформаційному впливу, для України актуальною проблемою є виявлення та блокування сепаратистських Інтернет-ресурсів, які використовуються представниками терористичних організацій квазіутворень на території держави в інтересах пропаганди ідеології, що закликає до повалення конституційного ладу в Україні, відокремлення її територій, екстремізму та тероризму.

За результатами вивчення експертних напрацювань встановлено, що підвищенню ефективності протидії використанню мережі Інтернет з метою здійснення деструктивних інформаційних впливів сприятимуть:

– цільове застосування положень Конвенції Ради Європи про кіберзлочинність щодо процедури направлення запи-

¹ М. Пілат, Інформаційні впливи та інформаційні війни: сутність понять та їхній взаємозв'язок в інформаційну епоху (2013) 32 *Вісник Львівського університету*. Серія міжнародні відносини 187.

² М. Дем'яненко, Досвід НАТО зі створення ефективної системи інформаційно-психологічної боротьби (2017) 23 *Резонанс* 3–17 <<http://nbuviap.gov.ua/images/rezonans/2017/rez23.pdf>> дата звернення 10.12.2023.

тів про взаємну допомогу за відсутності відповідних міжнародних угод, а також норм законодавства про боротьбу з тероризмом до випадків кібертероризму (положення Конвенції Ради Європи про запобігання тероризму, що стосуються публічного підбурювання до вчинення терористичного злочину);

- встановлення жорсткої правової відповідальності як стримуючого фактору для осіб, які приймають участь у підготовці та здійсненні терористичних актів;

- вдосконалення захисту мереж з метою унеможливлення доступу зловмисників до її вразливих компонентів;

- системний аналіз кіберпростору для виявлення і розуміння існуючих і прогнозованих загроз;

- обмін розвідувальними даними щодо протидії загрозам використання кіберпростору в терористичних цілях;

- обмеження публічного висвітлення успішно проведених кібертерористичних атак.

Таким чином, дієвість протидії деструктивним інформаційним впливам, при реалізації яких використовуються сучасні інформаційні технології, залежить від темпів імплементації міжнародного досвіду правового регулювання процесів в інформаційній сфері, рівня правозастосовної діяльності у боротьбі з цим негативним явищем, а також науково-технічного забезпечення суб'єктів, що здійснюють відповідні контрзаходи.

Висновки. Широкомасштабні і динамічні перетворення, що відбуваються в інформаційній сфері в умовах інформаційної війни проти України, характеризуються цілеспрямованим використанням агресором деструктивного інформаційного впливу, який супроводжується проведенням противником спеціальних інформаційних операцій із задіянням потужного арсеналу сил і засобів. Наслідки цих дій можуть мати довгострокову і короткострокову перспективу у контексті нанесення шкоди державному суверенітету, територіальній цілісності, секто-

ру безпеки і оборони та, у цілому, всім складовим національної безпеки України. Крім цього, агресор спрямовує свої зусилля на підлив міжнародного іміджу України, її добросусідських відносин та конкурентної спроможності у різних галузях (аграрна, металургійна, оборонно-промислова, транспортних перевезень) на регіональних і світових ринках, компрометує досягнення у сфері використання ІТ-технологій.

Суттєвим загрозам від такого впливу підвергається на сьогодні внутрішній інформаційний простір України, уразливими місцями якого є національна ідея, культура і наукові досягнення, суспільна думка, свідомість населення, ставлення українців до країн-сусідів та засоби масової інформації.

Деструктивний інформаційний вплив на Україну може здійснюватись з боку агресора (противника), його союзників і регіональних квазіутворень із застосуванням комплексного підходу. Він також може бути багатовекторним (зосередженість відразу на декількох напрямках застосування – політика, економіка, засоби масової інформації тощо) і одновекторним (сфера безпеки і оборони).

Враховуючи мультидисциплінарний характер досліджуваної проблематики, вважаємо, що способи протидії деструктивним інформаційним впливам, які реалізуються в ході інформаційної війни, повинні бути «гібридними». У реаліях сьогодення Україна разом із світовою спільнотою та країнами-партнерами вживає заходів з протидії цьому негативному явищу в усіх життєво важливих сферах забезпечення національної безпеки держави. При цьому, шляхами підвищення ефективності боротьби з агресором в інформаційній сфері є взаємообмін профільними науковими напрацюваннями і практичним досвідом, всебічне та своєчасне інформаційно-аналітичне, методичне і технологічне забезпечення задіяних у протидії державних інституцій.

REFERENCES

BIBLIOGRAPHY

ARTICLES

1. Chernysh R, Sotsialni mrezhi, yak odyn iz instrumentiv nakopychennia ta protypravnoho vykorystannia personalnykh danykh hromadian [Social networks as one of the tools of accumulation and illegal use of personal data of citizens] (2017) 136 *Problemy zakonnosti* 205–214 [in Ukrainian].
2. Chernysh R, Feik, yak odyn iz instrumentiv nehatyvnoho vplyvu na natsionalnu bezpeku Ukrainy v umovakh vedennia hibrydnoi viiny [Fake, as one of the instruments of negative influence on the national security of Ukraine in the conditions of conducting a hybrid war] (2019) 2 *Chasopys kyivskoho universytetu prava* 109–114 <http://kul.kiev.ua/doc/chasopys2019/CHAS_19_2.pdf> data zvernennia 05.12.2023 [in Ukrainian].
3. Chernysh R, Orhanizatsiini ta pravovi metody protydii manipuluvanniu svidomistiu hromadian u sotsialnykh mrezhakh [Organizational and legal methods of countering the manipulation of citizens' consciousness in social networks] (2020) 3–4 *Visnyk kryminalnoho sudochynstva* 168–177 [in Ukrainian].
4. Chernysh R, Ihnatiuk M, Zaritskyi O, Protydiia destruktyvnomu informatsiinomu vplyvu v Ukraini: pravovi ta orhanizatsiini aspekty [Countering destructive information influence in Ukraine: legal and organizational aspects] (2022) 1 *Yurydychnyi naukovi elektronnyi zhurnal* <<http://www.lsej.org.ua/index.php/arkhiv-numeriv?id=146>> data zvernennia 04.12.2023 [in Ukrainian].
5. Dem'ianenko M, Dosvid NATO zi stvorennia efektyvnoi systemy informatsiino-psykholohichnoi borotby [NATO's experience in creating an effective system of information and psychological warfare] (2017) 23 *Rezonans* 3–17 <<http://nbuviap.gov.ua/images/rezonans/2017/rez23.pdf>> data zvernennia 10.12.2023 [in Ukrainian].
6. Dokladno pro vyznachennia poniattia informatsii ta vykorystannia yii v diialnosti pravookhoronnykh orhaniv ta spetssluzhb dyv: Pohoretskyi M A, Operativno-rozshukova informatsiia: do vyznachennia poniattia [Operational investigative information: to the definition of the concept] (2007) 36 *Visnyk Kharkivskoho nats. un-tu vnutr. sprav* 13–19 [in Ukrainian].
7. Malyk Ya, Informatsiina viina i Ukraina [Information Wars and Ukraine] (2015) 15 *Naukovi visnyk* [in Ukrainian].
8. Petryk V, Sutnist informatsiinoi bezpeky derzhavy, suspilstva ta osoby [The essence of information security of the state, society and the individual] (2009) *Yurydychnyi zhurnal* <<http://www.justinian.com.ua/article.php?id=3222>> data zvernennia 05.12.2023 [in Ukrainian].
9. Pilat M, Informatsiini vplyvy ta informatsiini viiny: sutnist poniat ta yikhni zviazozv'iazok v informatsiinu epokhu [Information influences and information wars: the essence of concepts and their relationship in the information age] (2013) 32 *Visnyk Lvivskoho universytetu Serii mizhnarodni vidnosyny* 187 [in Ukrainian].
10. Pohoretskyi M, Shelomentsev V, Poniattia kiberprostoru yak seredovyscha vchynnennia zlochyniv [The concept of cyberspace as an environment for committing crimes] (2009) 2 *Informatsiina bezpeka liudyny, suspilstva, derzhavy* 77–81 [in Ukrainian].
11. Pohoretskyi M, Shelomentsev V, Kiberzlochyny: do vyznachennia poniattia [Cybercrimes: to define the concept] (2012) 8 *Visnyk prokuratury* 89–96 [in Ukrainian].
12. Pohoretskyi M, Cherniak A, Serhieieva D, Chernysh R ta Toporetska Z, Detection and proof of cybercrime (2022) 11(53) *Amazonia Investiga* 259–269 data zvernennia 08.12.2023 [in Ukrainian].
13. Pohoretskyi M, Shelomentsev V, Pravove zabezpechennia borotby z kiberzlochynamy v Ukraini: problemni pytannia [Legal support for combating cybercrime in Ukraine: problematic issues] (2011) 8 (122) *Visnyk prokuratury* 30–38 [in Ukrainian].
14. Pohoretskyi M A, Operativno-rozshukova informatsiia: do vyznachennia poniattia [Operational-Search Information: Towards a Definition] (2007) 36 *Visnyk Kharkivskoho nats. un-tu vnutr. sprav* 13–19.
15. Sviderska O, Tsyfrova propahanda ta ryzyky informatsiinoi bezpeky u konteksti rosiisko-ukrainskoi viiny [Digital Propaganda and Information Security Risks in the Context of the Russian-Ukrainian War] *Naukovi zhurnal «Politykus»* <<http://politicus.od.ua/>> data zvernennia 09.12.2023 [in Ukrainian].

BOOKS

16. Dulles A, *The Secret Surrender*. Harper & Row [The Secret Surrender. Harper & Row] (1966) <https://books.google.de/books/about/The_Secret_Surrender.html?id=b3kNAAAAIAAJ&redir_esc=y> data zvernennia 06.12.2023 [in Ukrainian].
17. Fromm E, *Vitecha vid svobody* [Escape from freedom] (Kharkiv, Knyzhkovyi Klub «Klub Simeinoho Dozvillia», 2019) 288 [in Ukrainian].

18. Pohoretskyi M A, *Operatyvno-rozshukova informatsiia* [Operational investigative information] *Mizhnarodna politseiska entsyklopediia: u 10 t. T. VI: Operatyvno-rozshukova diialnist politsii (militsii) / vidp. red. V V Kovalenko, Ye V Moiseiev, V Ya Tatsii, Yu S Shemshuchenko* (Kyiv, Atika, 2010) 570–572 [in Ukrainian].
19. Libicki M, *What is information warfare?* [What is information war?] (Washington, National Defense University Press, 1995) 104 <http://www.dodccrp.org/files/Libicki_What_Is.pdf> data zvernennia 08.12.2023 [in Ukrainian].
20. Ron T, *Weapon Systems and Information War* [Weapons Systems and Information Warfare] (Boeing Aerospace Co. Seattle, WA, 1976) <https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf> data zvernennia 07.12.2023 [in Ukrainian].

Chernysh R. F.,
Candidate of Law, Associate Professor,
National Academy of Security Service of Ukraine
ORCID ID: 0000-0003-4176-7569

DOI: <https://doi.org/10.17721/2413-5372.2023.3-4/205-214>

DESTRUCTIVE INFORMATION INFLUENCE AS AN ELEMENT OF INFORMATION WARFARE

«The essence of any war is deception! «
Sun Tzu

Annotation. The article stated that from the moment Ukraine was declared an independent state, a rapid transition from totalitarianism to democracy began. However, in addition to positive changes, there are also certain negative points that may threaten national sovereignty against the background of the war unleashed by the Russian Federation. This was also facilitated by the support of military aggression by individual citizens, which is due to the purposeful influence on their (primarily young) consciousness and subconsciousness and the formation of an anti-social position (distrust of the current authorities, law enforcement and special agencies, the Armed Forces of Ukraine, etc.), as well as incitement to commit acts of disobedience or other illegal actions. This happens, including, as a result of the implementation of systemic destructive influence.

Taking into account the above, **the purpose of the article** is to analyze the concept of «destructive» and outline the organizational and legal methods of countering this negative phenomenon (including on the Internet).

Attention has been drawn to the fact that the systematic and complex disinformation organized by the special services of the Russian Federation is currently an actual threat to the state sovereignty and territorial integrity of Ukraine. The above requires improvement of: legal regulation of information dissemination, the procedure for restricting access to it in cases of fakeness; methods and legal grounds for prosecuting subjects involved in disseminating disinformation.

It is argued that the destructive informational influence that accompanies external armed aggression and is implemented in the internal informational space of Ukraine aims to strengthen anti-Ukrainian positions through purposeful pressure on state institutions, polarizing society and replacing traditional national values. In the context of countering such influence, the discussion is spreading regarding: the limits of state intervention in the information sphere, since democracy can exist only in the presence of strong and independent mass media, guaranteeing everyone the right to freedom of speech and expression of their views; observance of democratic principles in the context of opposing weapons of the so-called «mass information destruction».

In the final part of the study, based on the results of the study of expert work, a number of measures are determined, the implementation of which will increase the effectiveness of countering the use of the Internet for the purpose of destructive informational influences.

Key words: destructive information influence, information war, the Internet, countermeasures against destructive information influence.