УДК 351.746:007

Зіновій Коваль
доцент кафедри права і законотворчого процесу
ОРІДУ НАДУ при Президентові України, к.держ.упр.

ДЕРЖАВНЕ УПРАВЛІННЯ СФЕРОЮ ІНФОРМАЦІЙНОЇ БОРОТЬБИ: ПІДХІД ДО ПОНЯТІЙНОГО АПАРАТУ

Публікація присвячена аналізу сучасних дискусійних наукових підходів до уточнення існуючих й наведення нових визначень щодо понятійного апарату управління сферою інформаційної боротьби України. Запропоновано уточнену цілісну систему понятійного апарату форм інформаційної боротьби відповідно до доктринальних інформаційних напрямів у визначених сферах суспільного життя.
Ключові слова: *інформаційна атака, інформаційна акція, інформаційний удар, інформаційна операція, інформаційна кампанія, інформаційна війна, інформаційно-психологічна та інформаційно-технічна операція, інформаційний напрям, інформаційний вплив.*

Zinoviy Koval

STATE ADMINISTRATION OF INFORMATIONAL WARFARE: APPROACH TO CONCEPTUAL MECHANISM

This publication is devoted to analysis of modern discussion scientific approaches to refinement of present and new definitions of conceptual mechanism of informational warfare state governing in Ukraine. Refined integral system of conceptual mechanism is proposed in accordance with doctrinal informational directions in different spheres of social life.
Keywords: *informational attack, informational action, informational impact, informational operation, informational campaign, informational war, informational-technical and informational-psychological operations, informational directions, informational influence.*

Зиновий Коваль

ГОСУДАРСТВЕННОЕ УПРАВЛЕНИЕ СФЕРОЙ ИНФОРМАЦИОННОЙ БОРЬБЫ: ПОДХОД К ПОНЯТИЙНОМУ АППАРАТУ

Публикация посвящена анализу современных дискуссионных научных подходов к уточнению существующих и приведению новых определений понятийного аппарата управления сферой информационной борьбы Украины. Предложена уточненная целостная система понятийного аппарата форм информационной борьбы в соответствии с доктринальными информационными направлениями в определенных сферах общественной жизни.
Ключевые слова: *информационная атака, информационная акция, информационный удар, информационная операция, информационная кампания, информационная война, информационно-психологическая и информационно-техническая операции, информационное направление, информационное влияние.*

Постановка проблеми

В теорії державного та воєнного управління все ще не вироблено єдиного підходу до визначень щодо понятійного апарату управління сферою інформаційної боротьби. Виникає необхідність додаткового аналізу окремих концептуальних підходів до запропонованих визначень та продовження дискусії щодо визначення цілісної системи форм ведення Україною інформаційної боротьби.

Аналіз останніх досліджень і публікацій

Дана проблематика обговорюється в періодичних друкованих виданнях та в мережі Інтернет. У наукових публікаціях цієї теми торкались: професор О. В. Левченко, фахівці Національного університету оборони України ім. І. Черняховського (НУОУ) А. О. Рось, Т. М. Дзюба, О. П. Дузь-Крятченко під керівництвом В. М. Телелима, з російських науковців – А. А. Ноговіцин та ін.

Виділення невирішених раніше частин загальної проблеми

Підходи до наукового аналізу визначень щодо понятійного апарату державного управління сферою інформаційної боротьби України все ще різняться, бачення їх різнопланові, концептуально неузгоджені тому потребують додаткового опрацювання. Давно настав час визначити цілісну систему форм ведення Україною інформаційної боротьби.

Мета

Мета даної публікації – аналіз окремих визначень понятійного апарату державного та воєнного управління сферою інформаційної боротьби України і напрацювання варіанту цілісної системи форм ведення Україною інформаційної боротьби.

Виклад основного матеріалу

У зв'язку зі стрімким розвитком інформаційних технологій та їх масовим застосуванням у різних галузях діяльності людства, зокрема в управлінській та військовій сфері, виникло таке принципово нове поняття, як «інформаційна боротьба», а слідом за ним − ціла низка похідних понять: «інформаційна війна», «інформаційна кампанія», «інформаційна операція» тощо. В умовах інформаційної революції нові терміни стали популярними, ними широко користуються в повсякденній діяльності науковці, політики, громадські діячі та журналісти. Застосовують нові поняття і спеціалісти інформаційної сфери національної безпеки нашої держави, але через відсутність загальноприйнятого понятійного апарату вони вживають ці терміни на власний розсуд, що часто викликає непорозуміння з боку інших фахівців. Нині, як зазначає український фахівець у справі інформаційної боротьби професор О. В. Левченко, гостро стоїть проблема відсутності єдиного понятійного апарату в інформаційній сфері національної безпеки нашої держави. Сутність такої класифікації полягає в наданні певній сукупності виявлених інформаційних заходів конкретної форми. При цьому спеціалісти, аналізуючи виявлені за-

ходи іноземного інформаційного впливу, роблять висновок: чи є це інформаційною акцією, інформаційною операцією чи інформаційною кампанією тощо. Саме тому О. В. Левченко порушує актуальну проблему розробки єдиного понятійного апарату, який був би максимально придатний для практичного застосування та пропонує визначення основних термінів, розроблених на основі аналізу й поєднання теоретичних і практичних підходів за цим напрямом. Він констатує, що у спеціальній літературі наводяться такі форми інформаційної боротьби, як «інформаційна війна», «інформаційна операція», «інформаційна кампанія,», «інформаційна атака», «інформаційний вплив», «інформаційна акція», але при цьому виявляються різні підходи до переліку зазначених форм, їх трактування й ранжування. [6] У справі формулювання понять сфери інформаційного протиборства успіхів досягли фахівці Національного університету оборони України ім. І. Черняховського (НУОУ) А. О. Рось, Т. М. Дзюба, О. П. Дузь-Крятченко та інші, які під керівництвом В. М. Телелима зробили спробу узагальнити понятійний апарат у «Словнику основних термінів у галузі інформаційної безпеки держави у воєнній сфері» [8].

Автор статті ставить перед собою завдання узагальнити, доповнити та систематизувати визначення форм інформаційної боротьби, запропонованих професором О. В. Левченком відповідно до Доктрини інформаційної безпеки України і напрацювання варіанту цілісної системи форм ведення Україною інформаційної боротьби.

Розпочати доречно з такого терміна, як «інформаційний захід», який прийнято характеризувати як елементарну короткочасну цілеспрямовану інформаційну дію деструктивного характеру на поодинокий об'єкт впливу на одному інформаційному напрямі. Інформаційні заходи можуть бути як психологічного, так і технічного характеру. Перші спрямовуються на свідомість і підсвідомість людей. Прикладами таких заходів можна вважати провокативне новинне Інтернет-повідомлення чи статтю замовного характеру у впливових ЗМІ, виступ державного діяча на прес-конференції, мітингу, радіо, телебаченні з оприлюдненням певної антиукраїнської тези тощо. Другі спрямовані на комп'ютерні, телекомунікаційні системи, інформаційні ресурси тощо. Як, наприклад, несанкціоноване проникнення до електронної бази даних урядової установи чи впровадження шкідливого програмного забезпечення в комп'ютерну мережу визначеного органу військового управління. Отже, інформаційний захід − це первинна інформаційна дія, що може мати подвійну спрямованість (інформаційно-технічну та інформаційно-психологічну) і яка реалізовується у восьми сферах життєдіяльності держави (зов-нішньополітичній, воєнній, внутрішньополітичній, економічній, соціальній та гуманітарній, науково-технологічній, екологічній), що визначені в Доктрині інформаційної безпеки України.

Державна управлінська політика у сфері забезпечення інформаційної безпеки України, відповідно до Доктрини інформаційної безпеки України, повинна бути зосереджена на конструктивному поєднанні діяльності держави, громадянського суспільства і людини за трьома головними напрямами: інформаційно-психологічному, технологічному та захисту інформації [5]. Отже, інформаційним напрям − один із визначених у Доктрині інформаційної безпеки України напрямів у зовнішньополітичній, воєнній, внутрішньополітичній, економічній, соціальній, гуманітарній, науково-технологічній та інших сферах життєдіяльності держави, за якими можуть реалізовуватися інформаційні загрози національній безпеці України. Відповідно до Доктрини інформаційної безпеки України, завданням на інформаційно-психологічному напрямі діяльності органів виконавчої влади є забезпечення конституційних прав і свобод людини і громадянина, створення сприятливого психологічного клімату в національному інформаційному просторі для утвердження загальнолюдських та національних моральних цінностей. Звертає на себе увагу відсутність конкретних завдань щодо організації комплексної інформаційно-психологічної протидії деструктивному зовнішньому та внутрішньому інформаційно-психологічному впливу.

Необхідно ввести ще одну категорію інформаційної боротьби: інформаційний вплив, який також доречно ділити на інформаційно-психологічний та інформаційно-технічний і визначати його як метод (засіб) інформаційного заходу щодо впливу суб'єкта інформаційної боротьби на відповідний об'єкт.

Отже, для наукового опису організації інформаційної боротьби (протидії) необхідні три первинні категорії: інформаційний захід через інформаційний вплив (атака, акція, удар, операція, кампанія, війна); інформаційний напрям (психологічний, технічний, захист інформації) та сам інформаційний вплив (технічний, психологічний). Інформаційний захід виступає як первинна інформаційно-організаційна дія, інформаційний напрям як цілевказ для інформаційної дії, а інформаційний вплив як метод (засіб) інформаційного заходу (інформаційної дії). Вся ця конструкція узагальнена та систематизована автором згідно з вимогами Доктрини інформаційної безпеки України.

Також необхідно визначитись з формами інформаційних заходів та уточнити їх сутність. Першою формою інформаційного заходу доречно визнати інформаційну атаку та характеризувати її (за О. В. Левченком) як сукупність кількох взаємопов'язаних прихованих інформаційних заходів, короткочасно спрямованих на один об'єкт впливу за певним інформаційним напрямом у визначеній сфері, що мають технічний/психологічний характер і за інтенсивністю можуть бути як вибірковими, так і масованими.

Друга форма інформаційного заходу – це інформаційна акція, яка характеризується сукупністю взаємопов'язаних більш масштабних інформаційно-психологічних заходів, які спрямовуються на один об'єкт впливу за певним інформаційним напрямом у визначеній сфері і проводяться протягом певного часу та мають психологічний/технічний характер і спрямовуються проти особи, певних соціальних груп населення, суспільства та його еліти.

Третя форма інформаційного заходу – це інформаційний удар. Інформаційний удар – це сукупність скоординованих масових та короткочасних узгоджених інформаційних (технічних/психологічних) атак, спрямованих на один чи кілька найважливіших елементів систем державного й військового управління супротивника у поєднанні, в деяких випадках, із заходами силового впливу на об'єкти з метою їх дезорганізації або виведення з ладу. Інформаційні удари зазвичай проводяться для отримання інформаційної переваги над супротивником на початку та під час збройної боротьби. Об'єктами інформаційних ударів можуть бути елементи інформаційної інфраструктури, систем теле-комунікації, управління, важливі інформаційні засоби, органи управління.

Четвертою формою інформаційного заходу доречно визначити інформаційну операцію. Інформаційна операція − це сукупність узгоджених та взаємопов'язаних за метою, завданнями, об'єктами впливу й часом інформаційних атак, акцій і ударів, котрі проводяться як послідовно, так і одночасно в одній обраній сфері життєді-

яльності держави. У мирний час метою інформаційних операцій може бути вплив на морально-психологічний стан вищого державного керівництва країни-супротивника і певних соціальних груп населення для схилення їх до прийняття рішень та дій у потрібному для протилежної держави напрямі. У воєнний час цілі інформаційних операцій полягають у дезорганізації системи державного управління та систем управління військами і зброєю, знищенні інформаційної інфраструктури супротивника, завоюванні інформаційної переваги над ним та створенні сприятливих умов в інформаційному просторі для дій своїх військ, а також у забезпеченні захисту власної інформаційної інфраструктури та інших складових інформаційного середовища від дій супротивника. Інформаційні операції можуть тривати від декількох тижнів до кількох місяців та можуть мати як чітко виражену психологічну або технічну спрямованість, так і поєднувати одночасно заходи психологічного й технічного впливу. Інформаційну операцію психологічної спрямованості традиційно називають інформаційно-психологічною операцією. Теоретично така операція ведеться шляхом організації лише заходів інформаційно-психологічного впливу. О. В. Левченко вважає, що в реальних умовах інформаційного протиборства в особливий період у рамках однієї операції, окрім заходів інформаційно-психологічного впливу, мають організовуватися й заходи активного, у тому числі інформаційно-технічного впливу на супротивника, фактично вестимуться не інформаційно-психологічні, а інформаційні операції, тому вважати інформаційно-психологічну операцію окремою формою інформаційної боротьби немає сенсу.

Автор цієї статті не поділяє цю думку й підтримує точку зору деяких вітчизняних науковців про те що інформаційно-технічні та інформаційно-психологічні операції можуть виступати самостійними формами інформаційної боротьби й проводитися незалежно одна від одної, відповідно до поставлених органами державного та військового управління завдань. Доречніше говорити, що інформаційно-психологічна операція є різ-новидом інформаційної операції поряд з інформаційно-технічною.

Водночас О. В. Левченко вказує на еволюцію поглядів іноземних військових фахівців на місце, роль та співвідношення інформаційно-психологічної операції і інформаційної операції, підкреслюючи, що військові спеціалісти низки провідних країн світу, насамперед США, дедалі більше відходять від уживання терміна «інформаційно-психологічна операція» та повсюди впроваджують термін «інформаційна операція». При цьому вважається, що інформаційна операція є основною формою інформаційної боротьби, а інформаційно-психологічні дії проводяться в її рамках на тактичному рівні. Більше того, в останній редакції польового статуту збройних сил США з організації та ведення інформаційних операцій FM 3-13 Inform and Influence Activities від 25 січня 2013 р. термін «інформаційно-психологічна операція» взагалі не використовується [1].

На переконання автора цієї статті, термін «інформаційно-психологічна операція» перестав використовуватись деякими країнами тому, що є велике бажання приховати саме психологічний характер деструктивного впливу як ефективний вражаючий чинник; що інформаційно-психологічні операції успішно проводяться й на стратегічному рівні, і що саме інструментами інформаційно-психологічної операції можна досягнути стратегічного успіху не переходячи до фази «гарячої війни».

Щодо терміну «спеціальних інформаційних операцій», то автор даної статті, на відміну від точки зору О. В. Левченка, вважає за доцільним залишити цей термін як різновид самостійних разових інформаційних операцій, що проводяться різними спецслужбами держави у мирний час чи загрозливий період з можливим застосуванням нетрадиційних засобів боротьби (елементів парапсихології, масового гіпнозу, нових спецзасобів та сил).

П'ятою формою інформаційного заходу доречно вважати інформаційну кампанію. Інформаційна кампанія, за О. В. Левченком, − це сукупність узгоджених та взаємопов'язаних за метою, завданнями, об'єктами впливу і часом інформаційних операцій, ударів, акцій і атак, котрі проводяться як послідовно, так і одночасно в кількох сферах життєдіяльності держави з метою сприяння досягнення визначених цілей власної національної політики. Основний об'єкт впливу інформаційної кампанії − це держава супротивника загалом, а кінцевою метою її проведення може бути встановлення повного контролю над зовнішньою та внутрішньою політикою протилежної країни. Інформаційна кампанія має, як правило, довготерміновий перманентний характер, вона може тривати роками (століттями – релігійні інформаційні кампанії) до досягнення, або недосягнення своєї кінцевої мети. Вона може посилюватися або згасати залежно від початку чи закінчення інформаційних операцій, ударів або окремих інформаційних акцій, які її складають. У рамках однієї інформаційної кампанії можуть одночасно або послідовно проводитися кілька інформаційних операцій, кожна з яких має власну сферу спрямування (зовнішньополітичну, внутрішньополітичну, економічну, військово-технічну тощо) й мету, яка разом з тим є частковою метою всієї кампанії. Автор даної статті погоджується з тим, що некоректно застосувати термін «інформаційна кампанія» до різного роду малозначущих інформаційних подій, заходів та акцій, як це часто роблять вітчизняні журналісти в засобах масової інформації.

Особливу увагу слід звернути на поняття «інформаційна війна» як шосту, завершальну форму інформаційних заходів. Під інформаційною війною у воєнній сфері доречно розуміти інформаційне протиборство, яке охоплює весь інформаційний простір ворогуючих держав і ведеться загалом в інтересах руйнування основ національної самосвідомості й державного устрою супротивника. Основне завдання інформаційної війни між державами – здійснення безпосереднього негативного руйнівного впливу на сукупну політичну могутність держави шляхом послаблення її реальних і потенційних можливостей щодо забезпечення власної безпеки, створення труднощів у внутрішньому розвитку і проведенні активної зовнішньої діяльності, завдання шкоди політичному іміджу держави. Головний об'єкт, на якому концентрується деструктивний інформаційний вплив у межах заходів інформаційної війни – громадська думка та свідомість окремої людини. Відомо, що термін «інформаційна війна» був запроваджений та активно використовувався з кінця минулого століття американськими військовими фахівцями, які донедавна називали інформаційну війну найвищою формою інформаційного протиборства. О. В. Левченко вважає, що це стосувалося того протиборства, яке здатні вести сучасними силами й засобами лише США та деякі інші провідні країни світу, а для умов української дійсності, можливостей держави та її Збройних Сил для ведення інформаційного протиборства у формі інформаційної війни є недостатньо. Та на думку автора цієї статті, такі можливості будуть і в України за умови концентрації усіх державних, громадських та приватних засобів інформаційного впливу під єдиним керівництвом. О. В. Левченко також вважає, що термін «інформаційна війна» слід від-

носити не до форм ведення інформаційної боротьби, а до загальних концептуальних понять, якими описується сучасна збройна боротьба за участю провідних країн світу. Такої позиції дотримуються і провідні російські військові теоретики [7]. Тому О. В. Левченко переконаний щодо недоцільності включення терміну «інформаційна війна» в нормативні документи ЗСУ зі значенням форми ведення ними інформаційної боротьби (протидії).

Навпаки, автор цієї статті наполягає на доцільності включення терміна «інформаційна війна» в нормативні документи не тільки ЗСУ, а й загальнодержавні та міжнародні. Інформаційна війна – це комплекс інформаційно-технічних та інформаційно-психологічних кампаній, окремих операцій, ударів, акцій, атак узгоджених та взаємопов'язаних за метою, завданнями, об'єктами впливу й часом, котрі проводяться як послідовно, так і одночасно в багатьох сферах життєдіяльності держави. Інформаційна війна може вестись перманентно, століттями і нести цивілізаційний характер. А те, що військові фахівці США останнім часом відійшли від уживання в оперативних (бойових) і нормативних документах категорії «інформаційна війна», тільки підтверджує думку про те, що зроблено це з метою уникнення самого терміну «війна», замінивши його більш нейтральною категорією «інформаційні операції» [2].

Мартін Лібікі – один із провідних теоретиків у галузі інформаційних війн – у своїй книзі «Що таке інформаційна війна», яка є класикою, визначає 7 форм інформаційної війни: командно-управлінська (націлена на знищення каналів зв'язку); розвідувальна (збір важливої і захист власної інформації); психологічна (пропаганда, інформаційна обробка населення, деморалізація); хакерська (диверсійні дії та атаки проти ворога шляхом створення спеціальних програм); економічна (інформаційна блокада й інформаційний імперіалізм); електронна (спрямована проти засобів електронних комунікацій – радіозв'язку, радарів, комп'ютерних мереж); кібервійна (Лібікі відокремив кібервійну від хакерської війни, вбачаючи в «кібервоїні» істоту, яка селиться в систему і живе в ній) [4]. Як бачимо, шість форм інформаційної війни із семи, за Мартіном Лібікі, належать до інформаційно-технічної сфери, одна – до інформаційно-психологічної. Отже видно, що термін «інформаційна війна» є доречним та міжнародно визнаним. Ще у 2009 році американський військовий дослідник Д. Ласіка, характеризуючи особливості «гібридної війни», був переконаний, що основою їх ведення є саме інформаційно-психологічна складова, а об'єктом впливу стає насамперед суспільна свідомість, а за нею − збройні сили та інфраструктура [3]. «Гібридна війна» широко використовує, в залежності від обставин, всі форми інформаційних заходів, особливо форму інформаційної війни.

Отже, у систему форм ведення інформаційної боротьби доцільно включати поряд з інформаційною кампанією, операцією, ударом, акцією, атакою й інформаційну війну. Звичайно, ці форми мають тісний взаємозв'язок і певну ієрархію. Найнижчою формою інформаційної боротьби в такій системі є інформаційна атака, найвищою − інформаційна війна. Західні фахівці вже однозначно назвали інформаційну війну найвищою формою ідеологічного протиборства. Як випливає з визначень, саме інформаційна війна як вид холодної війни (технічної та психологічної) є найвищою формою інформаційної боротьби, а її проведення сприяє досягненню стратегічних цілей у протиборстві двох держав (союзів держав). Основу кожної з наведених форм інформаційної боротьби становлять інформаційні заходи, які плануються і проводяться системно й у визначеній сукупності утворюють інформаційну кампанію, операцію, атаку, акцію чи удар.

Таким чином, багато в чому погоджуючись з точкою зору О. В. Левченка, для подальшого використання у вітчизняних нормативних документах та практичній діяльності автор пропонує свою цілісну систему форм ведення інформаційної боротьби: найвищою її формою є інформаційна війна; у її рамках проводяться інформаційні кампанії, операції та удари; складовими інформаційної операції є інформаційні акції та атаки; нижчою формою є інформаційна атака, яку утворює певна сукупність інформаційних заходів. Цілком можливе також ситуативне проведення окремих інформаційних кампаній, операцій, акцій та атак, які спрямовуються на вирішення завдань, котрі раптово виникають під час ведення інформаційної боротьби як у мирний, так і у воєнний час. Графічне зображення співвідношення названих форм у сутності феномену інформаційної боротьби в системі національної безпеки України наведене автором на рис. 1.

Висновки

З метою узгодженого підходу до розуміння інформаційної боротьби необхідним є запровадження єдиного понятійного апарату в інформаційній сфері національної безпеки нашої держави. Доречно погодитись з точкою зору професора О. В. Левченка, що інформаційний захід − це первинна узагальнена інформаційна дія. Інформаційний захід може мати потрійну спрямованість: інформаційно-технічну та інформаційно-психологічну та захисту інформації і реалізовуватись у восьми сферах життєдіяльності держави (зовнішньополітичній, воєнній, внутрішньополітичній, економічній, соціальній та гуманітарній, науково-технологічній, екологічній), що визначені в Доктрині інформаційної безпеки України.

Для наукового опису організації інформаційної боротьби (протидії) необхідні три первинні категорії: інформаційний захід (атака, акція, удар, операція, кампанія, війна); інформаційний напрям (психологічний, технічний, захисту інформації) та інформаційний вплив (технічний, психологічний). Інформаційний захід виступає як первинна інформаційно-організаційна дія, інформаційний напрям − як цілевказ для інформаційної дії та інформаційний вплив як метод (засіб) інформаційного заходу (інформаційної дії). Вся ця конструкція узагальнена та систематизована автором відповідно до вимог Доктрини інформаційної безпеки України.

Автор цієї статті наполягає на доцільності включення терміну «інформаційна війна» в нормативні документи не тільки ЗСУ, а й загальнодержавні й міжнародні та пропонує визначити інформаційну війну як комплекс інформаційно-технічних та інформаційно-психологічних кампаній, окремих операцій, ударів, акцій, атак, узгоджених та взаємопов'язаних за метою, завданнями, об'єктами впливу й часом, котрі проводяться як послідовно, так і одночасно в багатьох сферах життєдіяльності держави. Інформаційна війна може вестись перманентно, століттями і нести цивілізаційний характер.

Тому доцільно у систему форм ведення інформаційної боротьби включати порід із інформаційною кампанією, операцією, ударом, акцією, атакою й інформаційну війну. Ці форми мають тісний взаємозв'язок і певну ієрархію. Найнижчою формою інформаційної боротьби в такій системі є інформаційна атака, найвищою − інформаційна війна. Як випливає з визначень, саме інформаційна війна як вид холодної війни (технічної та психологічної) є найвищою формою інформаційної боротьби, а її проведення сприяє досягненню стратегіч-

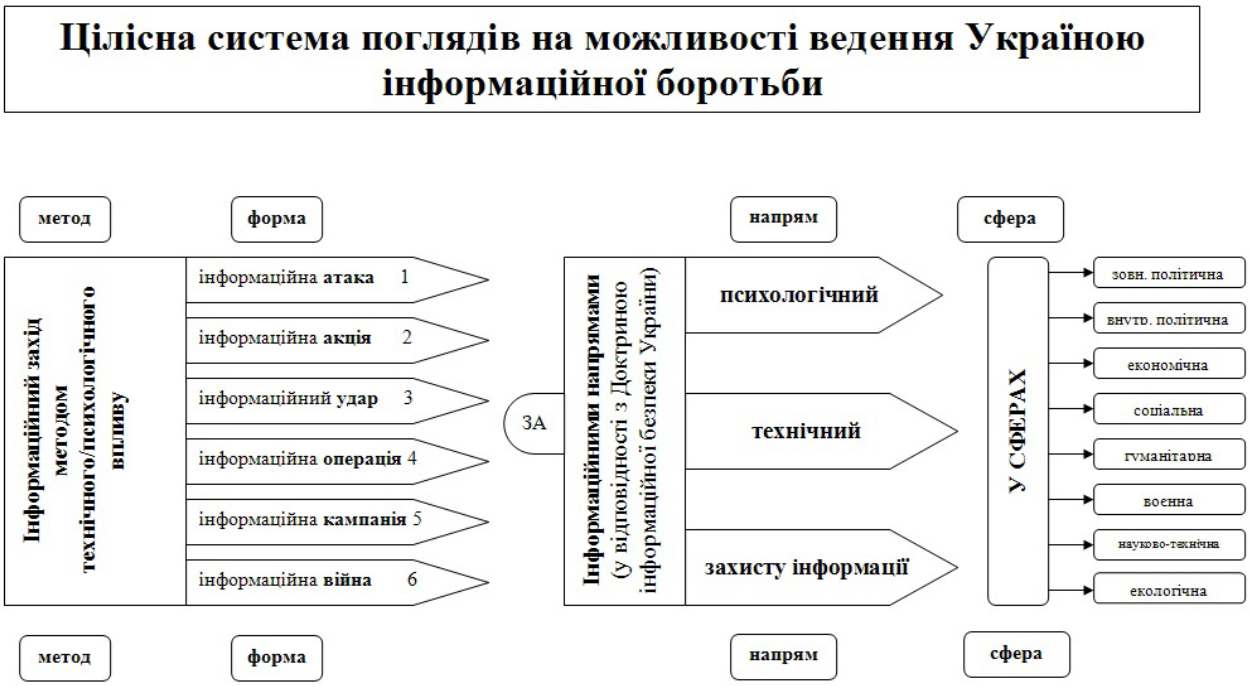

Рис. 1. Цілісна система поглядів на можливості ведення Україною інформаційної боротьби

них цілей у протиборстві двох держав (союзів держав). Таким чином, погоджуючись багато в чому з точкою зору О. В. Левченка, для подальшого використання у вітчизняних нормативних документах та практичній діяльності автор пропонує наступну цілісну систему форм ведення інформаційної боротьби: найвищою її формою є інформаційна війна; у її рамках проводяться інформаційні кампанії, операції та удари; складовими інформаційної операції є інформаційні акції та атаки; нижчою формою є інформаційна атака, яку утворює певна сукупність інформаційних заходів. Цілком можливе також ситуативне проведення окремих інформаційних кампаній, операцій, акцій та атак, які спрямовуються на вирішення завдань, котрі раптово виникають під час ведення інформаційної боротьби як у мирний, так і у воєнний час.

На відміну від точки зору О. В. Левченка, автор цієї статті вважає за доцільне залишити термін «спеціальні інформаційні операції» як різновид самостійних разових інформаційних операцій, що проводяться різними спецслужбами держави у мирний час чи загрозливий період з можливим застосуванням нетрадиційних засобів боротьби (елементів парапсихології, масового гіпнозу, нових спецзасобів та сил).

Література.

1. Field Manual 3-13, Inform and Influence Activities, Department of the Army, 25 January 2013 [Електронний ресурс]. − Режим доступу: http://www.armypubs.army.mil/doc- trine/DR_pubs/dr_a/pdf/fm3_13.pdf.

2. Joint Publication 3 - 13, Joint Doctrine for Information Operations, Department of Defence USA, 1998 [Електронний ресурс]. − Режим доступу: http://www.c4i.org/jp3_13.pdf.

3. Lasica D.T. Strategic Implication of Hybrid War: A Theory of Victory: Monograph / D.T.Lasica. – USA, 2009 - [Електронний ресурс]. − Режим доступу: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA513663.

4. Martin C.Libicki. What is informational warfare? - Washington, D.C., 1995. - [Електронний ресурс]. − Режим доступу: www.dodccrp.org/files/Libicki_What_is.pdf.

5. Доктрина інформаційної безпеки України [затверджена указом Президента України від 8 липня 2009 р. № 514/2009]. − К. : Офіційний вісник України, 2009. − № 52.

6. Левченко О. В. Форми ведення інформаційної боротьби: практичний підхід до понятійного апарату. // Наука і оборона. − № 3. – 2013. – С. 21−26.

7. Ноговицын А. А. В центре внимания − информационная безопасность / А. А. Ноговицын // Красная звезда. – 27.02. 2009. − С. 3.

8. Словник основних термінів у галузі інформаційної безпеки держави у воєнній сфері / [уклад. А. Рось та ін.]; за ред. М. Телелима. − К. : НУОУ, 2012. − 54 с.