УДК 340.1
DOI https://doi.org/10.32838/1606-3716/2019.3/06

Шемчук В.В.
Таврійський національний університет імені В.І. Вернадського

КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО РОЗУМІННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ В СУЧАСНОМУ СВІТІ

У статі проаналізовані основні підходи до розуміння сутності інформаційних воєн, виділено їх специфіку. Обґрунтовано власне визначення інформаційної війни як соціально-політичного явища. Вона зазвичай посягає на світоглядні цінності, сприяє деморалізації та фрагментації населення держав-противників у межах глобального інформаційного простору. Запропоновано удосконалити правові основи протидії та попередження інформаційних війн на національному рівні в Україні. Тому важливо вивчати зарубіжний досвід, відповідні доктринальні та нормативні джерела з метою пошуку оптимальних шляхів виходу з такої ситуації.

Ключові слова: *інформаційна війна, інформаційне протиборство, інформаційний простір, правова основа, попередження, протидія, інформаційна безпека.*

Постановка проблеми. Перехід держави до інформаційного суспільства вимагає переосмислення, в окремих випадках і розробки нових механізмів регулювання відносин, що виникають між громадянами, їх об'єднаннями та державою. Усі суб'єкти інформаційних відносин повинні усвідомлювати й виконувати свою роль у цьому процесі, але саме держава покликана активно впливати на ці трансформаційні процеси, залучати до співпраці політиків, науковців, практиків, міжнародних експертів і громадськість.

Водночас події, які відбуваються в Україні, в останні декілька років демонструють появу нових викликів і загроз у даній сфері. Зокрема, особливої уваги заслуговують різні форми впливу, протиборства тощо. З розвитком та впровадженням сучасних інформаційних технологій практично в усі сфери нашого життя зростає рівень загроз несанкціонованого доступу в процес роботи систем та витоку важливої інформації. Технічний прогрес суттєво впливає на вирішення військових, торговельних, економічних конфліктів, унаслідок чого силові методи іноді поступаються інформаційним.

Тому прикметно, що змінилось традиційне чи класичне розуміння війни. В інформаційному просторі національного і міжнародного масштабів ведуться інформаційні атаки та інформаційні війни. Слід відзначити, що практично в усіх збройних конфліктах за останні десятиліття ефективно використовувалися методи та засоби інформаційної боротьби, які можуть призвести до таких трагічних наслідків, як: зміна суспільного ладу і політичного устрою; розпад держави; втрата армії; розвал економічної системи в країні; страта національної ідеї та духовних цінностей; загибель людей тощо [1].

Аналіз останніх досліджень і публікацій. Проблематику інформаційних впливів та протиборств, інформаційних війн неодноразово порушували і вичвалали вітчизняні та зарубіжні дослідники. Тут варто відзначити таких учених, як: Дж. Арквілли, Р. Гула, Г. Почепцов, Н. Камінська, Г. Карпенко, Я. Короход, І. Костюк, Д. Кюль, М. Лібікі, С. Любарський, Р. Моландер, Дж. Най, В. Остроухов, С. Расторгуєв, О. Саприкін, Г. Сасин, О. Сивак, П. Ткачук, П. Шевчук, О. Цуканова, В. Хорошко, Ю. Хохлачова, О. Щурко та інші.

Разом із тим неоднозначне розуміння згаданих категорій, іноді їх ототожнення змушують і надалі привернути увагу, особливо щодо з'ясування їхньої суті, а також правових основ їх попередження і протидії.

Постановка завдання. Отже, мета статті передбачає вивчення і виокремлення різних підходів до визначення і розуміння інформаційних війн, виділення їх специфіки, обґрунтування власних визначень. На основі цього важливо сформулювати відповідні пропозиції до визначення ефективних способів їх протидії.

Виклад основного матеріалу дослідження. Інформаційні війни як явище існували в тій чи іншій мірі з давніх часів. Історичний розвиток людства свідчить про те, що поняття «інформаційна війна» завжди супроводжувало та визначало разом зі зброєю хід, характер і результат воєн, битв, операцій.

Видатний китайський військовий теоретик Сун-Цзи у VI–V ст. до н.е. вперше запропонував використовувати інформаційні заходи як альтернативу бойовим діям. Він сформулював дев'ять заповідей, дотримання яких забезпечувало такий потужний вплив на духовний світ армії противника, що вона просто «розкладалася» ще до початку битви. Сун-Цзи зазначав, що «у війні, як правило, найкраща політика зводиться до захоплення держави цілісною <...> Здобути сотню перемог у боях – це не вершина мистецтва. Підкорити суперника без бою – ось вінець мистецтва» [2, с. 40]. Основні ідеї Суньцзи активно розвивали й інші китайські мислителі. Зокрема, військовий теоретик Чжуге Лян (III ст. н.е.). вважав, що «у воєнних діях атака на психіку – головне завдання. Психологічна війна – це головне, бій – це другорядна справа». Не абсолютизував збройне насильство і відомий прусський воєнний теоретик К. Клаузевіц, автор класичного визначення поняття «війна»: «Доведеться хоч не хоч визнавати й такі війни, які полягають лише в погрозі супротивнику» [3, с. 231]. Вперше термін «інформаційна війна» був використаний в 1985 р. у Китаї Шень Вейгуаном.

Здійснення інформаційних впливів з використанням інформаційної зброї (приховування інформації; подача її частково, в певному ракурсі; перебільшення наслідків) було зафіксовано літописцями на теренах України ще за Київської Русі. Так, загальновідомим є факт поїздки княгині Ольги до Константинополя, проте ні візантійські, ні руські джерела не висвітлюють причину та мету подолання такого довгого шляху. Войовничий князь Святослав заздалегідь повідомляв противника про свій похід, проте залишалися таємницею напрям та сили, котрі планувалося задіяти. Це давало можливість навести паніку в стані військ та швидко розгромити противника [4, с. 18].

В інформаційному просторі України тривалий час спостерігається боротьба за управління ресурсами, вплив і контроль на території нашої держави. Події з кінця 2013 – початку 2014 рр. стали драматичними для України. Внаслідок дестабілізації внутрішньої політичної ситуації, експансії Криму та «гібридної війни» на сході України змінилася геополітична ситуація як у Європі, так і фактично в усьому світі.

Це, на нашу думку, потребує з'ясування природи й сутності таких, видається, споріднених категорій, як інформаційна війна, інформаційний вплив, експансія, гібридна війна, електронна війна, хакерська війна, мережева війна, кібервійна, консцієнтальна війна, психологічна війна, інформаційне протиборство тощо.

Так, одним із перших у відкритому друці, хто написав про феномен інформаційних воєн, був М. Маклюєн у 1960 роках. Уже тоді було відомо, що «холодна війна» ведеться за допомогою інформаційних технологій, оскільки у всі часи війни велися за допомогою передових технологій. Дослідник відмітив, що якщо «гарячі» війни минулого використовували зброю, знищуючи ворогів одного за іншим, то інформаційна зброя за допомогою телебачення та кіно, навпаки, занурює все населення в певний світ уяви: «земна куля тепер – не більше, ніж село» [5, с. 7].

Інформаційна війна є тотальним явищем, де неможливим є визначення його початку та кінця. Зокрема, на думку С. Расторгуєва, інформаційна війна – це наявність боротьби між державами за допомогою інформаційної зброї, тобто це відкриті та приховані цілеспрямовані інформаційні впливи систем (держав) одна на одну з метою отримання переваги в матеріальній сфері, де інформаційні впливи – це впливи за допомогою таких засобів, використання яких дозволяє досягати задуманих цілей [6, с. 455–456].

Можна погодитись з думкою О. Саприкіна, що інформаційна експансія є технологією набагато місткішою, ніж «інформаційна війна» або «інформаційна атака». Ці терміни можна вважати складниками інформаційної експансії. Інформаційна експансія – система, що склалася в засобах інформації розвинених держав, і методи, що використані для пропагандистського забезпечення певних геополітичних цілей [7, с. 40].

У листопаді 1991 р., аналізуючи досвід досягнення інформаційної переваги після операції «Буря в пустелі», генерал Гленн Отіс, колишній командувач Командування сухопутних військ США з навчання та доктрин, опублікував роботу, в який стверджував, що «природа війни повністю змінилася. Та сторона, яка виграє інформаційну війну, – переможе <…> інформація є ключем до сучасної війни – у стратегічному, оперативному, тактичному і технічному планах». Офіційно визначеним термін «інформаційна війна» як комплексне спільне застосування сил і засобів інформаційної боротьби та збройної боротьби (при домінуванні засобів інформаційної боротьби) вперше став

у керівних документах США, зокрема в директиві МО США Т 3600.1 від 12 грудня 1992 р., під назвою «Інформаційна війна» [8].

У сучасному науковому дискурсі проблемі вивчення такого надскладного соціально-політичного явища, як «інформаційна війна», надається достатньо уваги. Різноманітність підходів до визначення основного змісту, відсутність єдиної системи класифікації призвели до унеможливлення створення уніфікованої дефініції понять інформаційної війни та інформаційно-політичного простору, відсутність методологічного осмислення співвідношення цих понять тощо.

Наприклад, А. Манойло зміст поняття інформаційної війни розглядає на різних рівнях пізнання: як соціальне явище; як поле політичних конфліктів; як особливу форма політичного конфлікту; як інструмент інформаційної політики [9]. А. Фісун до цього додає ще й форму психологічного впливу [10, с. 534].

Найбільш важливими, як відзначають Хорошко В. та Хохлачова Ю., є електронна та психологічна війни. Електронна війна об'єктом свого впливу має засоби електронних комунікацій – радіозв'язок, телевізійні та комп'ютерні мережі. Психологічна війна здійснюється шляхом пропаганди, «промивання мозку» та іншими методами інформаційної обробки населення. Далі згадані автори виділяють інформаційну війну, безліч визначень якої пов'язано зі складністю і багатогранністю такого явища, труднощами побудови аналогій із традиційними війнами. Якщо спробувати трансформувати визначення в поняття «інформаційна війна», то навряд чи щось конструктивне вийде. Це пов'язано з рядом особливостей інформаційної війни [11; 12].

Загалом, у залежності від основних аспектів дослідження об'єкта, які вирізняють науковці, та від гіпотез щодо сутності явища виділяється шість основних підходів до поняття «інформаційна війна».

Так, *соціально-комунікативний* підхід трактує поняття інформаційної війни як сукупність окремих інформаційних заходів, інформаційних способів і засобів корпоративної конкуренції, що є продуктом еволюційного розвитку способів і засобів комунікації між людьми, суспільствами, державами та світом загалом. У межах цього підходу український дослідник Г.Г. Почепцов визначає «інформаційну війну» як всеосяжну, цілісну стратегію, яка надає значущості та цінності інформації в процесах командування, управління і виконання наказів збройними силами й реалізації національної політики [13, с. 3]. Особливостями соціально-комунікативного підходу є:

– відображення сутності досліджуваного явища лише як закономірного розвитку людського суспільства в межах біологічної еволюції з домінуванням принципів природного відбору, боротьби за існування й виживання найбільш пристосованих як визначальних факторів громадського життя;

– визначення природи соціального конфлікту як вічного та непереборного;

– трактування інформаційної агресії як нової трансформованої форми природної агресії людини.

Маніпулятивно-психологічний підхід визначає суть інформаційної війни як системи способів і засобів психологічного впливу на індивідуальну та масову свідомість з метою спрямування її у вигідному для суб'єкта впливу напрямі. Формами інформаційної війни є використання психотропної зброї, побудова віртуального світу, підміна реальності тощо. Представники цього підходу вважають, що інформаційно-психологічна війна – це вплив на суперника через засоби масового психологічного впливу для зміни світогляду чи ініціювання процесу самознищення, добровільної здачі території, ресурсів і т.п. [14]. Тобто специфічними особливостями цього підходу є:

– розкриття психологічного впливу феномена;

– комплексне розкриття психологічного аспекту і маніпулятивної природи інформаційної війни;

– ігнорування оборонного (захисного) характеру інформаційної війни;

– нівелювання технічного аспекту, матеріальних засобів інформаційного протиборства;

– недостатнє прогнозування наслідків впливу економічного складника.

Військово-прикладний підхід зараховує інформаційну агресію до сфери військового протиборства й розглядає її в комплексі спільного застосування сил і засобів інформаційної та збройної боротьби. При цьому представники військово-прикладного підходу не вважають інформаційну війну окремим методом ведення війни. На їхню думку, існує множина форм інформаційної війни, кожна з яких претендує на різні концепції, зокрема: командно-контрольні, розвідувальні війни; радіоелектронна боротьба; психологічні операції; хакерська війна, програмні атаки на інформаційні системи; інформаційно-економічна війна; кібервійни [15]. Кібервійну розглядають як процес розвитку та поширення інформаційних технологій. У військовій сфері – як комплексне використання висо-

коточної зброї, технологій «Стелс», бойових і розвідувальних засобів з урахуванням футуристичних розробок у галузі роботизації та автоматизації [16]. Характерними особливостями цього підходу є:

– системність, що дає можливість охопити політичний, економічний, психологічний та інший аспекти;

– «агресивний характер», зорієнтований на швидке досягнення бажаного тактичного результату з одночасною втратою стратегічної перспективи;

– ігнорування прогнозування наслідків для іншої сторони конфлікту;

– нівелювання соціального аспекту за домінування політичного складника конфлікту.

Державно-інструментальний підхід називає інформаційну війну інструментом зовнішньої та внутрішньої політики, «можливістю для збору, обробки та розповсюдження безперервного потоку інформації <…> у відповідь на дії противника» [17]. Особливістю цього підходу є абсолютизація ролі політичних інститутів і організації держави у веденні інформаційної війни та нівелювання впливу соціальних, економічних і психологічних чинників.

Геополітичний підхід. Дослідники вважають інформаційну війну явищем латентно мирного періоду міждержавного протиборства, що дозволяє вирішувати зовнішньополітичні завдання несиловими методами. Інформаційна війна стосується сфери геополітичного протиборства, її трактують як особливий вид відносин між державами, за якого для вирішення існуючих протиріч використовують методи, засоби й технології впливу на інформаційну сферу функціонування цих держав. Під інформаційною війною дослідники цього напряму розуміють дії, які спрямовані на завдання противнику конкретного, відчутного збитку в окремих галузях його діяльності [3, с. 481].

З-поміж характеристик цього підходу виокремимо такі:

– охоплення геополітичних суб'єктів інформаційно-політичного простору;

– трактування інформаційної війни як певного природного закону;

– ігнорування значимості особистості як окремого об'єкта для впливу;

– недостатнє вивчення причин інформаційної війни.

Віртуально-кібернетичний підхід. Інформаційна війна розглядається як сукупність технічних, програмних та інших засобів, які використовують у віртуальному просторі, з метою ураження інформаційних систем противника (комп'ютерні віруси та ін.). Кібервійна – елемент інформаційної війни, що здійснюється з використанням засобів всесвітньої мережі у формі кібератак. Сутність інформаційної війни полягає у застосуванні прихованих цілеспрямованих інформаційних впливів інформаційних систем одна на одну з метою одержання певного прибутку в матеріальній сфері [6, с. 51]. Наголошено на тому, що інформаційно-блогова або мережева війна – це внутрішньосередовищна особливість Інтернету, яка виявляється у формах жорсткої дискусії, цілковитого свавілля із взаємними образами, атаками на ресурси противника, зламами особистої інформації та ресурсів. Блоги стають потужним інструментом формування громадської думки [18, с. 3]. «Інформаційна війна, на думку американських теоретиків Дж. Аркуіла та Д. Ронфельдта, може бути частиною широкого та всеохоплюючого поняття ворожих дій – мережевої війни або кібервійни» [19].

Властивостями віртуально-кібернетичного підходу є:

– розкриття суті інформаційної війни крізь площину математичного виміру;

– виокремлення тенденцій сучасного інформаційного простору та розвитку інформаційних технологій (особливо в контексті інформаційно-блогових процесів);

– ігнорування психологічного аспекту явища;

– невизначеність ролі держави в цьому процесі;

– домінування теоретичного, а не практичного значення, відсутність рекомендацій та прийомів, які б дали змогу виявити інформаційну агресію і захиститись від неї.

Комплексний підхід. Український дослідник А. Фісун констатує, що жоден із зазначених підходів не розкриває сутність інформаційної війни комплексно ні як політичного конфлікту, ні як соціального явища, ні як соціокультурного феномену: «Інформаційна війна – це комплексний, відкритий чи прихований цілеспрямований інформаційний вплив однієї сторони, чи взаємний вплив сторін одна на одну, який містить систему методів і засобів впливу на людей, їхню психіку та поведінку, на інформаційні ресурси та інформаційні системи, з метою досягнення інформаційної переваги (в забезпеченні національної стратегії), що зумовлює прийняття сприятливих для ініціатора впливу рішень або знищення інформаційної інфраструктури противника, з одночасним зміцненням і захистом власної інформації та інформаційних систем» [10, с. 538].

На нашу думку, до комплексного підходу слід зарахувати й дефініцію В. Ліпкана, Ю. Максименко,

В. Желіховського: «Інформаційна війна – це: 1) дії, розпочаті для досягнення інформаційної переваги шляхом завдання шкоди інформації, процесам, що базуються на інформації та інформаційних системах супротивника за одночасного захисту власної інформації, процесів, що базуються на інформації та інформаційних системах; 2) нефізична атака на інформацію, інформаційні процеси та інформаційну інфраструктуру; 3) найвищий ступінь інформаційного протиборства, спрямований на розв'язання суспільно-політичних, ідеологічних, національних, територіальних та інших конфліктів між державами, народами, націями, класами й соціальними групами шляхом широкомасштабної реалізації засобів і методів інформаційного насильства (інформаційної зброї)» [20, с. 270].

В ідеологіях маргінальних політичних формувань екстремістського та окультистського напрямів став популярним так званий *конспірологічний* підхід. Найбільш послідовним апологетом цього напряму можна вважати О.Г. Дугіна. Інформаційну війну він розглядає як форму тотального впливу глобальних політичних, економічних, терористичних, сектантських мережевих структур (хасидсько-парамасонська група, Захід на чолі з США, країни «золотого мільярду») з метою контролювання політичної, соціальної, економічної ситуації та інтенсифікації трансформаційних тенденцій духовності світового суспільства через спрямування інформаційних процесів в інтересах США, які одночасно створюють систему захисту власного мережевого коду, який ці процеси дешифрує та структурує.

Сегментами глобальної мережі в цьому підході є:

– пряме проамериканське лобі експертів, політологів, аналітиків, технологів, які контролюють владу та претендують на роль інтелектуальної еліти суспільства;

– представники великого бізнесу та політичної еліти, які орієнтовані на фінансово-економічну діяльність за кордоном;

– ЗМІ та ЗМК, які виконують функцію масованого інформаційного впливу за допомогою потоків візуальної та смислової інформації.

Тобто, «інформаційну війну ведуть ідейні кілери — найманці з числа політиків, духівництва, інтелектуалів, які зраджують інтересам народу, проституюючи совість і розум». Характерною рисою «мережевої війни», за О.Г. Дугіним, є тотальний інформаційний вплив «мережевої п'ятої колони» «агентів впливу» – рушійної сили світового заколоту з метою десуверенізації країни [21]. Особливостями цього підходу є:

– дослідження мережевого характеру сучасного світового бізнесу, політичних проектів, терористичних формувань і сектантських організацій;

– розкриття сутності діяльності «агентів впливу»;

– надмірна абсолютизація поняття «мережі», ігнорування психологічних особливостей людини як самостійного індивіда;

– містично-конспірологічний погляд на роль світових глобальних структур, демонізація західного світу, захоплення ідеєю «світового єврейського заколоту», окультизм і расовий фактор.

Інформаційна війна здійснюється у формі інформаційного протиборства як системи цілеспрямованих дії для створення інформаційної переваги, за допомогою руйнування інформації, інформаційних систем протилежної сторони, при цьому одночасно відбувається процес захисту власної інформації та інформаційних систем [22–23].

Висновки. Отже, на нашу думку, *інформаційна війна* – це суспільно-політичне явище, яке у *політичному аспекті* є продовженням домінуючих ідеологічних засад державної політики, що здійснюється за допомогою комплексу засобів інформаційно-технологічної індустрії, механізмів інформаційно-психологічного впливу на суспільство всередині держави чи населення країн-конкурентів в умовах політичного (воєнно-політичного, економічного) конфлікту з метою формування в *соціальному аспекті* єдності суспільства, визначення його ідентичності та інформаційного захисту світоглядних цінностей, а також – деморалізації та фрагментації населення і силової компоненти держав-противників у межах глобального інформаційного простору.

Інформаційна війна як явище деструктивно впливає на розвиток інформаційних суспільств та одночасно сприяє розвитку практично всіх пріоритетних сфер життєдіяльності, у т. ч., через вплив маніпулятивних технологій, що використовуються в інформаційних війнах, на світову політику тощо. Світові тенденції розвитку державно-правових явищ потребують не тільки удосконалення форм і методів державного управління, але й нових стратегій забезпечення національної інформаційної безпеки. З огляду на це важливо вдосконалити правові основи протидії та попередження інформаційних війн, негативного інформаційно-психологічного впливу на національному рівні в Україні. Для цього важливо вивчати як зарубіжний досвід, так і відповідні доктринальні та нормативні джерела з метою пошуку оптимальних шляхів виходу з тих ситуацій, в яких опинилось українське суспільство в останні роки.

Список літератури:

1. Сасин Г.В. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір. *ГРАНІ*. 2015. № 3 (119) С. 18–23.
2. Сун-Цзы, У-Цзы. Трактаты о военном искусстве. Москва : АСТ, 2002. 558 с.
3. Манойло А.В., Петренко А.И., Фролов Д.П. Государственная информационная политика в условиях информационно-психологической войны. Москва : Горячая линия Телеком, 2009. 541 с.
4. Гуз А.М. Історія захисту інформації в Україні та провідних країнах світу : навчальний посіб. Київ : КНТ, 2007. 260 с.
5. Маклюэн М. Понимание Медиа: Внешние расширения человека ; пер. с англ. В. Николаева ; Москва ; Жуковский : «КАНОН-пресс-Ц», «Кучково поле», 2003. 464 с.
6. Расторгуев С.П. Философия информационной войны. Москва : Московский психолого-социальный институт, 2003. 496 с.
7. Саприкін О. Інформаційна експансія, інформаційна війна та інформаційна атака у засобах масової інформації на прикладі Євро-2012. *Вісник Книжкової палати.* 2013. № 1. С. 40–43.
8. Adams J. The Next World War. Computers Are the Weapons and the Front Line Is Everywhere. NewYork, 1998. 368 p.
9. Манойло А.В. Управление психологической войной URL: http://andreymanoylo. vov. ru/ uprpsiv.html
10. Фісун А.О. Ґенеза поняття «інформаційна війна». *Гілея*. 2011. № 49. С. 534–538.
11. Іванченко І.С. Забезпечення інформаційної безпеки держави. Київ : ПВП «Задруга», 2013. 170 с.
12. Хорошко В.О., Хохлачова Ю.Є. Інформаційна війна. ЗМІ як інструмент інформаційного впливу на суспільство. 2016. Т. 22. Частина 1: Безпека інформації. DOI: 10.18372/2225-5036.22.11104
13. Почепцов Г.Г. Информационные войны. Москва : Рефл-бук ; Киев : Ваклер, 2000. 576 с.
14. Морозов А.М. От физической к психологической войне. Эволюция форм войны в процессе развития цивилизации. URL: http://psyfactor.org/biowar.htm
15. Libicki M. What is Information Warfare? URL: http://www.iwar.org.uk/iwar/resources/ndu/infowar/a003cont.html
16. Климчук О.О., Кравченко Р.М. Кібервійна у сучасних умовах. *Інформаційна безпека. Людина. Суспільство. Держава.* 2011. № 1 (5). С. 78–84.
17. Yoshihara T. Chinese Information Warfare: A Phantom Menace or Emerging Threat? Strategic Studies Institute, U.S. Army War College. 43 p.
18. Жаров М., Шевяков Т. Хроники информационной войны. Москва : Европа, 2009. 48 с.
19. Arquilla J. Ronfeldt D. Cyber war is Coming! Comparative Strategy 2 (April-June 1993). URL: http://www.rand.org/ pubs/reprints/RP223.html
20. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах євроінтеграції : навч. посібник. Київ : КНТ, 2006. 280 с.
21. Дугин А.Г. Сетевые войны. Доклад на заседании Изборского клуба 08.07.2013 г. URL: http://dynacon.ru/content/articles/2318
22. Ткачук П.П. та ін. Інформаційна війна і національна безпека : монографія. Львів : НАСВ, 2015. 265 с.
23. Любарський С.В. Місце та роль мережевої розвідки в моделях інформаційного протиборства. *Збірник наукових праць ВІТІ НТУУ «КПІ».* 2013. № 1. С. 31–39.

КОНЦЕПТУАЛЬНЫЕ ПОДХОДЫ К ПОНИМАНИЮ ИНФОРМАЦИОННОЙ ВОЙНЫ В СОВРЕМЕННОМ МИРЕ

В статье проанализированы основные подходы к пониманию сущности информационных войн, выделена их специфика. Обосновано собственное определение информационной войны как социально-политического явления. Она обычно посягает на мировоззренческие ценности, способствует деморализации и фрагментации населения государств-противников в пределах глобального информационного пространства. Предложено усовершенствовать правовые основы противодействия и предупреждения информационных войн на национальном уровне в Украине. Поэтому важно изучать зарубежный опыт, соответствующие доктринальные и нормативные источники с целью поиска оптимальных путей выхода из такой ситуации.

Ключевые слова: *информационная война, информационное противоборство, информационное пространство, правовая основа, предупреждение, противодействие, информационная безопасность.*

CONCEPTUAL APPROACHES TO THE UNDERSTANDING OF INFORMATION WARFARE IN THE MODERN WORLD

The article analyzes the basic approaches to understanding information wars, highlighted their specificity.

In modern the scientific discourse of problems difficult socio-political phenomenon of «information warfare» given enough attention. A variety of approaches to the definition of the main content, the lack of a unified system of classification led to prevent the creation of a uniform definition of concepts information war and political space, the lack of a methodological understanding correlation these concepts and others.

Substantiation of the definition of information warfare as socio-political phenomenon, reflecting the dominant ideological principles of the State policy realization using complex tools of the information-technology industry, the mechanisms of the information-psychological influence on society within or countries-competitors in terms of the military-political, economic or other conflicts with the purpose of forming an identity society, information protection of philosophical values, as well as demoralize thrown in and fragmentation of the population and power components of the States-opponents within the global information space.

Proposed to improve the legal basis for combating and prevention information warfare at the national level in Ukraine, therefore it is important to learn how foreign experience, appropriate doctrinal and legal sources with the aim of finding optimal ways out of this situation.

Key words: *information warfare, information past rivalry, ìnformation space, legal framework, prevention, counteraction, information security.*