DOI: 10.18372/2307-9061.59.15596
УДК 340:32.019.51(045)

В. Б. Череватюк,
кандидат історичних наук, доцент
ORCID ID: https://orcid.org/0000-0002-4077-206X

О. О. Бойко,
здобувач вищої освіти другого (магістерського) рівня

ІНФОРМАЦІЙНІ ВІЙНИ (КОНФЛІКТИ): ТЕОРЕТИКО-ПРАВОВИЙ АСПЕКТ

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

Мета: *в умовах стрімкого розвитку суспільства, технологій та засобів відтворення інформації гостро стоїть проблема протидії інформаційній війні. У статті автори проводять паралелі між звичною війною та інформаційною, зокрема визначають відмінності між цими явищами. Метою статті є дослідження теоретичних аспектів інформаційних війн (конфліктів), узагальнення пропозицій щодо протидії інформаційним війнам.* ***Методи:*** *методологічну основу дослідження склали загальнонаукові методи пізнання, порівняльно-правовий; соціологічний; логічний; діалектичний.* ***Результати:*** *проаналізовані основні методи ведення інформаційної війни, зокрема: підкуп; шантаж; залякування; маніпулювання свідомістю людей; погіршення політичної та економічної ситуації всередині країни; створення фіктивної опозиції; викрадення людей; організація та проведення терористичних актів тощо. Доведено, що створення контрпропаганди; розвиток засобів масової інформації; створення інформаційної коаліції; розвиток аналітичного мислення у громадян країни тощо є ефективними методами протидії інформаційним війнам.* ***Обговорення:*** *у даній статті автори розвивають думку про те, що новітній інформаційній зброї ми маємо протиставити іміджеву дипломатію, популяризацію бренду України у світовому просторі та ефективну політику, яка повинна реалізуватися через різні канали та засоби комунікації на міжнародній арені. Публічна дипломатія також є інструментом протидії гібридним загрозам, дезінформації та фейкам. Формування позитивного іміджу України у світі потребує тісної координації з усіма дотичними інституціями, як державними, так і недержавними.*

Ключові слова: *конфлікт; гібридна війна; інформаційна війна; інформаційна зброя; кіберконфлікти; методи протидії.*

Постановка проблеми та її актуальність. Дефініція «конфлікт» походить від латинського слова «conflictus», що в перекладі звучить як «ті, що зіштовхнулися». Традиційно, аналізуючи конфлікти, говорять про найбільш гострий спосіб вирішення протиріч у поглядах, цілях, інтересах, які виникають під час взаємодії людей один із одним. Сьогодні, в час інтенсивного впровадженням нових технологій, інноваційних процесів, соціальних змін у суспільстві, змінюються і види конфліктів, і виникають нові способи їх попередження і вирішення.

Для того, щоб ґрунтовно розібратися у суті таких понять як збройний конфлікт, інформаційна війна, гібридна війна, слід розуміти, що з розвитком технологій змінюються методи і способи їх ведення, по-іншому відбувається управління ними і зовсім непростим є їх вирішення. Так, розрізняють два види збройних конфліктів:

міжнародний збройний конфлікт (конфлікт між двома і більше державами) та збройний конфлікт неміжнародного характеру (конфлікт, що відбувається на території однієї держави, зіткнення неміжнародного характеру) [1]. Побутує думка, що у співвідношенні війна і збройний конфлікт, поняття «збройний конфлікт» є ширшим і включає саме поняття «війна». Але не кожний збройний конфлікт можна називати війною, оскільки між ними існує значна відмінність. А.П. Ладиненко вважає, що термін «війна» став дедалі частіше застовуватися до ситуацій, які не можуть кваліфікуватися як збройний конфлікт. Наприклад, інформаційна війна, ідеологічна війна, війна з тероризмом та ін. [2, с. 55].

У свою чергу, Мартін ван Кревельд передбачав, що війна в класичному розуміння взагалі перестане існувати у найближчому майбутньому, а їй на зміну прийдуть конфлікти низької інтенсивності, з бойовими сутичками, терактами, масовими вбивствами мирних громадян та тотальною пропагандою, що стане одним із ефективних елементів контролю за населенням [3, с. 308-309].

Яскравим прикладом видозміни війни є інформаційна війна. Інформаційна війна – це боротьба з використанням винятково інформаційного озброєння, тобто інформаційних технологій, які базуються на виробництві, розповсюдженні та нав'язуванні інформації. Інформаційна війна може характеризуватися як вид інформаційного протиборства та форма протиборства між суб'єктами, що передбачає інформаційний вплив на населення із використанням засобів масової інформації, комп'ютерних мереж тощо, з метою формування відповідної суспільної думки, підриву морального духу як усього суспільства, так і окремих його індивідів [4, с. 556-557].

Проблематика інформаційних війн достатньо широка та має кілька логічних підтем. У науковій, спеціалізованій та публіцистичній літературі відсутнє однозначне трактування цього феномена, а використовуються визначення, які застосовні до сучасного типу ведення війни, такі як: нелінійна (non-linearwar), не конвенційна (unconventionalwarfare), гібридна (hybridwarfare), змішана (compoundwarfare), нестандартна (irregularwarfare), «війна без лінії фронту» чи «конфлікт низької інтенсивності» [5, с. 49].

Сьогодні в світі відбувається все більше змін: наукових, інформаційних, технічних та технологічних. Нове покоління технологій стає ресурсом для ведення інформаційних воєн, розв'язування збройних конфліктів, маніпулювання державами та, що є більш важливим, маніпулювання життями людей.

Аналіз останніх досліджень і публікацій. Не дивлячись на значний інтерес до даної проблематики, можна констатувати, що у вітчизняній науці недостатньо ґрунтовно вивчене питання особливостей інформаційної та гібридної війни, так як зміни у цій сфері відбуваються дуже швидко. Такий вид конфліктів був предметом досліджень вітчизняних та зарубіжних авторів: В.М. Абакумов, Ю.О. Горбань, А.І. Баровська, М.А. Ожеван, Н.Ф. Семен, В.А. Ліпкан, І.М. Сопілко, О.В. Шевченко, Г.Г. Почепцов, О.В. Курбан, М. Рижков, В.П. Горбулін, О.Г. Додонов, Д.В. Ланде, Т.В. Коваленко, І.В. Владленова, Е.А. Кальницький, О.А. Лазоренко, В.К. Конах, В.Ф. Ткач, О.М. Косогов, А.О. Сірик, Л.Є. Смола, А. Манойло, А. Петренко, Д. Фролов та ін. Незважаючи на значну кількість досліджень, проблема регулювання та протидії інформаційним війнам не втрачає своєї актуальності.

Метою цієї статті є дослідження теоретичних аспектів інформаційних війн (конфліктів), узагальнення пропозицій щодо протидії інформаційним війнам.

Виклад основного матеріалу. Якщо прослідкувати еволюцію, то історія розвитку інформаційних війн – це історія розвитку людства, історія боротьби цивілізацій. Чимало прикладів перемоги і поразки в конкретних боях, коли ситуація різко змінювалася завдяки яким-небудь військовим хитрощам, цілеспрямованому поширенню дезінформації. Доведення інформації до певної особи або групи осіб і отримання від цього «профіту» – інформаційна операція, яка є елементом інформаційної війни. Так, наприклад, китайський воєначальник Сунь-Цзи в своєму трактаті «Мистецтво війни» першим узагальнив досвід інформаційного впливу на противника: «здобути сотню перемог у боях – це не межа ми-

стецтва. Підкорити супротивника без бою – ось вінець мистецтва». Сунь-Цзи мав на увазі саме інформаційні операції: «знищується все добре, що є в країні супротивника. Розпалюйте сварки і зіткнення серед громадян ворожої сторони» [6, с. 39].

Вагому роль у збройному протиборстві інформаційна війна почала відігравати із початку масових війн «машинної» ери. Вперше друковані засоби впливу на супротивника широко були застосовані в Першій світовій війні. Особливо активно ці засоби використовувалися Великобританією. Поширення пропагандистських листівок над позиціями німецьких військ несподівано дало ефект, і Лондон створив спеціальний орган для розробки інформаційних матеріалів, що містили британське трактування ведення війни. А наприкінці війни країни Антанти створили спеціальний штаб по морально-психологічному знищенню німецької армії, що також вплинуло на результат бойових дій. При цьому, до роботи цієї структури масово залучалися фахівці: письменники, художники, журналісти [7, с. 58].

Слушною є думка В. Дудка щодо того, що війна інформації на сьогодні стала одним із найнебезпечніших видів зброї, і основними її складовими можна вважати такі компоненти як: збір тактичної інформації; гарантування безпеки власних інформаційних ресурсів поширення пропаганди або дезінформації; підрив якості інформації супротивника і попередження можливості збору інформації супротивником [8]. Г.Г. Почепцов, проаналізувавши відмінності між звичайною війною та інформаційною, поділив їх на окремі блоки, зокрема: інформаційна війна має гнучкий арсенал озброєння та високу непередбачуваність; в інформаційній війні можливе тільки поетапне захоплення територій; в інформаційній війні є можливість багатократного захоплення тих самих людей (або окремих тематичних аспектів у їх свідомості), працює нечітка логіка; в інформаційній війні воюючі сторони неможливо виокремити за ознакою належності до якої-небудь групи або виконання певної соціальної ролі; в інформаційній війні вплив на супротивника невідчутний та може бути в доброзичливій формі; в інформаційній війні вплив вибірковий та охоплює оазні верстви населення по-різному; в інформаційній війні основною небезпекою є відсутність видимих руйнувань. У результаті захисні механізми суспільства не активуються [9, с. 38].

З огляду на ці відмінності, можна стверджувати, що основною проблемою інформаційної війни є її нетиповість та непередбачуваність. Також виникає складність із визначенням структури такого виду конфлікту, як інформаційна війна. Так, наприклад, якщо взяти звичну модель війни, то можна виділити основні складові конфлікту: учасники конфлікту, предмет і об'єкт конфлікту, умови, в яких відбувається конфлікт, та суб'єктивність сприйняття конфлікту. Інформаційна війна, в свою чергу, направлена на те, щоб структурні елементи конфлікту приховати, та, як це частіше буває, підмінити їх, створюючи неіснуючих учасників, створюючи неіснуючі ситуації тощо. Візьмемо до прикладу білоруський конфлікт, пов'язаний із примусовою за допомогою обману і погроз посадку літака Ryanair в аеропорту Мінська, який світова спільнота називає актом «повітряного піратства». При цьому сьогоднішній білоруський режим не нехтує ніякими засобами боротьби із власними критиками і цього разу він зазіхнув уже й на міжнародні норми. При цьому активно використовується і популяризується дезінформація про справжні причини посадки повітряного судна в Мінську.

У зв'язку із конфліктом на Сході України, анексією Криму Росією, ми уже давно перебуваємо у стані інформаційної війни. Інформаційна війна Росії проти України є чинником великої гібридної війни. Зважаючи на події останніх семи років, по відношенню до нас використовуються різні методи, які можна назвати інформаційною зброєю: підкуп; шантаж; залякування; маніпулювання свідомістю людей; погіршення політичної та економічної ситуації всередині країни; створення фіктивної опозиції; викрадення людей; організація та проведення терористичних актів тощо. Інформаційна зброя має багатоаспектну дію і вражає не тільки комп'ютерні мережі, канали цифрової комунікації, а й суспільну та індивідуальну свідомість.

У будь-якій війні є люди, яким війна вигідна. Для таких людей вітчизна буде там, де він буде «у виграші». Такі люди не мають принципів і вони є дуже хорошим провідником маніпулятивних пасток. На таких людях буде використовуватися перший метод – підкуп. За гроші вони готові говорити, а якщо потрібно, то і робити, такі речі, які хоча і будуть не відповідати дійсності, але з огляду, наприклад, на нестабільну ситуацію всередині країни, будуть мати вплив та ще більше «розхитувати» без того нестабільну ситуацію. У разі, коли ці люди проявляють бажання вийти з цієї гри, або зайняти протилежну сторону, ініціатор інформаційної війни починає використовувати наступний метод – шантажу. В таких випадках, проти цієї особи будуть використовувати її ж минуле, нагадуючи, що саме вона брала гроші та продавала свою державу, будуть будь-яким способом давати зрозуміти, що вже сторону змінити неможливо, будь створювати ілюзію вибору, де є тільки два шляхи: або ж ти працюєш на нас, або ж тебе, наприклад, звинувачують у державній зраді.

Розхитавши ситуацію всередині держави, починається маніпулювання свідомістю людей, шляхом використання дезінформації та створення так званого «самовтілюваного пророцтва», де люди, повіривши в дезінформацію, самі починають втілювати її в життя.

Для того, щоб підтримувати «необхідний клімат» в країні, ініціатору, як суб'єкту конфлікту, необхідно його постійно підсилювати, іншими словами – погіршувати політичну та економічну ситуацію. З цією метою ініціатор (суб'єкт) інформаційної війни буде шукати найбільш вразливі місця і влучати по них. Якщо в країні є проблеми з корупцією – на цьому буде активно акцентуватися увага і створюватися сприятливе середовище для підвищення рівня корупційних ризиків. Високий рівень корупції дестабілізує суспільство, підриває рівень довіри до влади, перешкоджає формуванню позитивного іміджу на міжнародній арені. Розвинені країни не бажають працювати з країною, яка погрузла в корупції, великий бізнес не хоче інвестувати та заходити на ринок такої держави. І як наслідок – створюється несприятлива економічна, а в подальшому і політична ситуація. У цей момент ініціатор (суб'єкт) інформаційної війни, який сприяв створенню даної ситуації, застосовує ще один вид інформаційної зброї – фіктивну опозицію, яка активно розвиває пропагандистську кампанію і обіцяє змінити все на краще.

Сьогодні сфера застосування інформаційної зброї, як вважає І.М. Харченко, включає як військову галузь, так і інші галузі потенційного використання з метою: дезорганізації діяльності управлінських структур, транспортних потоків та засобів комунікації; блокування діяльності окремих підприємств та банків, а також цільових галузей промисловості шляхом порушення технологічних зв'язків та системи взаєморозрахунків і т. ін.; ініціювання техногенних катастроф на території іншої сторони через порушення управління технологічними процесами та об'єктами; масового поширення у свідомості людей певних уявлень, поведінкових стереотипів; виклик невдоволення або паніки, а також провокування деструктивних дій різноманітних груп [10].

Правильно спланована інформаційна війна може закінчитися повним або частковим захопленням країни. Варто також зазначити, що сторін у цій війні може бути більше ніж дві. Часто буває, що країна, проти якої розгорнули інформаційну війну, може бути плацдармом для іншої інформаційної війни, більш глобальної. Причому терміни цієї війни необмежені. Підготовка стадій може займати і п'ять, і десять, і двадцять років.

На основі методів ведення інформаційної війни можна розробити методи протидії інформаційній війні. В Україні суб'єктами формування та реалізації політики в інформаційній сфері є: Рада національної безпеки і оборони України (далі – РНБО); Міністерство інформаційної політики України; Міністерство закордонних справ України; Міністерство оборони України; Державна служба спеціального зв'язку та захисту інформації України; поліція.

Варто також зазначити, що 14 травня 2021 р. РНБО ухвалила стратегію розвитку кібербезпеки на наступні 5 років. Також було зазначено, що 13 травня 2021 р. Міністерством цифрової трансформації було відкрито кіберцентр UA30, який

увійшов до структури Служби спецзв'язку та захисту інформації України. Очікується, що кіберцентр надаватиме послуги кіберзахисту, виявлення та реагування на кіберзагрози як для державних організацій, так і для пересічних громадян [11]. Секретарем РНБО Олексієм Даніловим також було повідомлено про створення кібервійськ України [12].

Методами протидії інформаційній війні, які також використовують згадані суб'єкти, зокрема, є: створення контрпропаганди; розвиток засобів масової інформації; створення інформаційної коаліції; розвиток аналітичного мислення у громадян країни тощо.

Контрпропаганда являє собою дискредитацію ідей супротивника, руйнування небажаних інформаційних сутностей та недопущення їх створення у майбутньому.

Розвиваючи ЗМІ, країна може вибрати два шляхи: перший – створення та розвиток ЗМІ, які будуть залежними від влади та знищення незалежних та пропагандистських ЗМІ супротивника, що є найбільш ефективним шляхом; другий – забезпечення реалізації можливостей для створення незалежних ЗМІ, які будуть висвітлювати фактичні дані, але в умовах інформаційної війни другий шлях неефективним, адже як казав Роберт Шеклі: «в інформаційній війні завжди програє той, хто каже правду, він обмежений правдою, брехун може казати все, що завгодно» [13].

Як і на будь-якій війні сторонам необхідні союзники – коаліція, яка буде протидіяти ворогам. В інформаційній війні ситуація аналогічна. Забезпечуючи собі коаліцію, країні відкриваються ширші можливості, зокрема, використання ЗМІ закордонних держав та, що також важливо, використання дипломатичних шляхів, наприклад, при вирішенні питання щодо ведення санкцій щодо ворожої країни.

Не менш важливим у протидії є розвиток аналітичного мислення у громадян країни. Забезпеченням розвитку аналітичного мислення потрібно займатися зі шкільних років людини, щоб у майбутньому, коли вона стане дорослою і зможе голосувати та вирішувати важливі питання, вона могла аналізувати ситуацію країни, ґрунтуючись не тільки на думці ЗМІ або конкретних осіб, а на особистому аналізі. Для людей, які вже сформовані, необхідно проводити, наприклад, регулярні тренінги за місцем роботи.

Метою інформаційної війни є послаблення моральних та матеріальних сил супротивника та посилення власних. Вона не призводить до кровопролиття чи вбивства, при її веденні немає жертв, вона знищує не населення, а державний механізм. Пам'ятаючи це, ми маємо навчитися протидіяти маніпулюванню нашою свідомістю, враховуючи, що в інформаційній війні психологічний вплив здійснюють різними засобами: військовими, економічними та політичними санкціями тощо.

Висновки. На підставі вищевикладеного можна зробити висновок про невирішеність питання щодо повноцінного забезпечення інструментарію протидії інформаційній війні. Ситуацію змінить розвиток технологій та способи донесення інформації. У цьому контексті варто розвивати існуючі та створювати нові інституції, які направлені на боротьбу з пропагандою та іншими методами ведення інформаційної війни. Новітній інформаційній зброї ми маємо протиставити іміджеву дипломатію, популяризацію бренду України у світовому просторі та ефективну політику, яка повинна реалізуватися через різні канали та засоби комунікації на міжнародній арені. Публічна дипломатія також є інструментом протидії гібридним загрозам, дезінформації та фейкам. Формування позитивного іміджу України у світі потребує тісної координації з усіма дотичними інституціями, як державними, так і недержавними

Також не менш ефективним методом протидії інформаційній війні є підвищення у суспільства аналітичних здібностей, навчання методам критичного аналізу повідомлень, убезпечення від інформаційних диверсій, підвищення рівня медіаграмотності. Для цього необхідно в закладах освіти усіх рівнів ввести навчальні дисципліни щодо інформаційної безпеки та інформаційної гігієни.

Література

1. Про затвердження інструкції про порядок виконання норм міжнародного гуманітарного права у Збройних Силах України: наказ

Міністерства оборони України від 23 бер. 2017 р. № 164, зареєстр. у Міністерстві юстиції України 09 чер. 2017 р. за № 704/30572. URL: https://zakon.rada.gov.ua/laws/show/z0704-17#Text

2. Нікітін А.А. Збройний конфлікт як вид воєнного конфлікту. *Науковий вісник Львівського державного університету внутрішніх справ.* 2018. № 2. URL: https://www.lvduvs.edu.ua/documents_pdf/visnyky/nvsy/nvsy_02_2018/08.pdf

3. Мартин ван Кревельд. Трансформация войны. Москва: ИРИСЭН, Мысль, 2011. 344 с. С. 308-309. URL: http://loveread.ec/view_global.php?id=44369

4. Правові засади розвитку інформаційного суспільства в Україні: монографія / В.А. Ліпкан, І.М. Сопілко, В.О. Кір'ян; за заг. ред. В.А. Ліпкана; Глоб. орг. союзн. лідерства, Акад. безпеки відкрит. сусп-ва, Акад. наук вищ. освіти України. Київ: ФОП Ліпкан О.С., 2015. 664 с. С. 556-557.

5. Смола Л.Є. Аспекти ведення інформаційної та гібридної війни в контексті застосування комунікаційних технологій. *S.P.A.C.E.* 2016. № 1. С. 48-53.

6. Сунь-цзи. Мистецтво війни / переклад Григорія Латника. Київ: Арій, 2014. 128 с.

7. Бойко О.О. Інформаційна війна в Україні в умовах сучасності. *Політ. Сучасні проблеми науки*: тези доповідей XIX Міжнар. наук. конф. молодих учених і студентів (м. Київ, 1-4 квіт. 2019 р.). Національний авіаційний університет. Київ: НАУ, 2019. С. 58.

8. Дудко В. Інформаційна війна проти України та методи її ведення. URL: http://www.polukr.net/uk/blog/2021/04/informacijna-vijna-proti-ukraini/

9. Почепцов Г.Г. Информационные войны. Москва, Киев: Рефл-бук, Ваклер, 2000. 576 с.

10. Харченко І.М., Сапогов С.О., Шамраєва В.М., Новікова Л.В. Основні засоби інформаційного протиборства та інформаційної війни як явища сучасного міжнародного політичного процесу. *Вісник Харківського національного університету імені В.Н. Каразіна*. 2017. URL: file:///C:/Users/ User/Downloads/9974-96-19803-1-10-20171219.pdf

11. UA30: в Україні відкрили кіберцентр для захисту від хакерських атак. *Радіо Свобода*. 2021. URL: https://www.radiosvoboda.org/a/ news-kiberzahyst-tsentr-ua30/31253744.html.

12. В Україні створять кібервійська. *Укрінформ*. 2021. URL: https://www. ukrinform.ua/ rubric-polytics/3245857-v-ukraini-stvorat-kibervijska-sekretar-rnbo.html.

13. Роберт Шекли о людях и информационных войнах: 11 цитат. URL: https://www.depo.ua/rus/svit/robert-shekli-o-prave-na-zhizn-haose-i-informatsionnyh-voynah-09122014000500

References

1. Pro zatverdzhennja instrukcii' pro porjadok vykonannja norm mizhnarodnogo gumanitarnogo prava u Zbrojnyh Sylah Ukrai'ny: nakaz Ministerstva oborony Ukrai'ny vid 23 ber. 2017 r. № 164, zarejestr. u Ministerstvi justycii' Ukrai'ny 09 cher. 2017 r. za № 704/30572. URL: https://zakon.rada.gov.ua/laws/show/z0704-17#Text

2. Nikitin A.A. Zbrojnyj konflikt jak vyd vojennogo konfliktu. *Naukovyj visnyk L'vivs'kogo derzhavnogo universytetu vnutrishnih sprav*. 2018. № 2. URL: https://www.lvduvs.edu.ua/ documents_pdf/visnyky/nvsy/nvsy_02_2018/08.pdf

3. Martin van Krevel'd. Transformacija vojny. Moskva: IRISJeN, Mysl', 2011. 344 s. S. 308-309. URL: http://loveread.ec/view_global.php?id=44369

4. Pravovi zasady rozvytku informacijnogo suspil'stva v Ukrai'ni: monografija / V.A. Lipkan, I.M. Sopilko, V.O. Kir'jan; za zag. red. V.A. Lipkana; Glob. org. sojuzn. liderstva, Akad. bezpeky vidkryt. susp-va, Akad. nauk vyshh. osvity Ukrai'ny. Kyi'v: FOP Lipkan O.S., 2015. 664 s. S. 556-557.

5. Smola L.Je. Aspekty vedennja informacijnoi' ta gibrydnoi' vijny v konteksti zastosuvannja komunikacijnyh tehnologij. *S.P.A.C.E.* 2016. № 1. S. 48-53.

6. Sun'-czy. Mystectvo vijny / pereklad Grygorija Latnyka. Kyi'v: Arij, 2014. 128 s.

7. Bojko O.O. Informacijna vijna v Ukrai'ni v umovah suchasnosti. *Polit. Suchasni problemy nauky*: tezy dopovidej XIX Mizhnar. nauk. konf. molodyh uchenyh i studentiv (m. Kyi'v, 1-4 kvit. 2019 r.). Nacional'nyj aviacijnyj universytet. Kyi'v: NAU, 2019. S. 58.

8. Dudko V. Informacijna vijna proty Ukrai'ny ta metody i'i' vedennja. URL: http://www.polukr.net/uk/blog/2021/04/informacijna-vijna-proti-ukraini/

9. Pochepcov G.G. Informacionnye vojny. Moskva, Kiev: Refl-buk, Vakler, 2000. 576 s.

10. Harchenko I.M., Sapogov S.O., Shamrajeva V.M., Novikova L.V. Osnovni zasoby informacijnogo protyborstva ta informacijnoi' vijny jak javyshha suchasnogo mizhnarodnogo politychnogo procesu. *Visnyk Harkivs'kogo nacional'nogo universytetu imeni V.N. Karazina*. 2017. URL: file:///C:/Users/ User/Downloads/ 9974-96-19803-1-10-20171219.pdf

11. UA30: v Ukrai'ni vidkryly kibercentr dlja zahystu vid hakers'kyh atak. *Radio Svoboda*. 2021. URL: https://www.radiosvoboda.org/a/news-kiberzahyst-tsentr-ua30/31253744.html.

12. V Ukrai'ni stvorjat' kibervijs'ka. *Ukrinform*. 2021. URL: https://www. ukrinform.ua/rubric-polytics/3245857-v-ukraini-stvorat-kibervijska-sekretar-rnbo.html.

13. Robert Shekli o ljudjah i informacionnyh vojnah: 11 citat. URL: https://www.depo.ua/rus/svit/robert-shekli-o-prave-na-zhizn-haose-i-informatsionnyh-voynah-09122014000500

V. Cherevatiuk, O. Boiko

INFORMATION WARS (CONFLICTS): THEORETICAL AND LEGAL ASPECT

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

Objective: *in the conditions of rapid development of society, technologies and means of reproduction of information, the problem of counteraction to information war is acute. In the article, the authors draw parallels between the usual war and information warfare, in particular, identify differences between these phenomena. The aim of the article is to study the theoretical aspects of information wars (conflicts), to generalize proposals for combating information wars.* ***Methods:*** *the methodological basis of the study were general scientific methods of cognition, comparative law; sociological; logical; dialectical.* ***Results:*** *the main methods of information warfare are analyzed, in particular: bribery; blackmail; intimidation; manipulation of people's consciousness; deterioration of the political and economic situation inside the country; creation of a fictitious opposition; kidnapping; organization and carrying out of terrorist acts, etc. It is proved that the creation of counter-propaganda; development of mass media; creation of an information coalition; development of analytical thinking in the citizens of the country, etc. are effective methods of counteracting information wars.* ***Discussion:*** *in this article, the authors develop the idea that we should oppose the latest information weapons to image diplomacy, promotion of the Ukrainian brand in the world and effective policies that should be implemented through various channels and means of communication in the international arena. Public diplomacy is also a tool to counter hybrid threats, misinformation and fakes. The formation of a positive image of Ukraine in the world requires close coordination with all relevant institutions, both state and non-state.*

Methods of counteracting the information war are: the creation of counter-propaganda; development of mass media; creation of an information coalition; development of analytical thinking in the citizens of the country, etc. Counter-propaganda is the discrediting of the enemy's ideas, the destruction of unwanted information entities and the prevention of their creation in the future. As in any war, the parties need allies - a coalition that will oppose the enemy. In the information war, the situation is similar. By securing a coalition, the country has greater opportunities, in particular, the use of foreign media and, more importantly, the use of diplomatic channels, for example, in resolving the issue of sanctions against an enemy country.

No less important in counteraction is the development of analytical thinking among the citizens of the country. Ensuring the development of analytical thinking should be done from school years, so that in the future, when they become adults and can vote and address important issues, they can analyze the situation based not only on the opinion of the media or individuals, but based on personal analysis. For people who are already formed, it is necessary to conduct, for example, regular training at the workplace.

Keywords: *conflicto; hybrid war; information war; information weapon; cyberconflicts; methods of counteraction.*