

УДК 355.488

ІНФОРМАЦІЙНА ЗБРОЯ І ПРАВОВІ ЗАСОБИ ІНФОРМАЦІЙНОЇ ВІЙНИ (НА ПРИКЛАДІ АКТУАЛЬНОЇ РОСІЙСЬКО-УКРАЇНСЬКОЇ ГІБРИДНОЇ ВІЙНИ Й ІНШИХ ВОЄН)

М. В. Головка

здобувач вищої освіти другого (магістерського) рівня спеціальності «Право»,
навчально-науковий інститут права

Науковий керівник – д.н.соц.ком., професор О. А. Мітчук

*Національний університет водного господарства та природокористування,
м. Рівне, Україна*

У статті з'ясовано функціонування інформаційної зброї і її правових засобів у веденні інформаційної війни. Визначено засоби інформаційної війни на прикладі актуальної російсько-української війни й інших воєн. Доведено, що інформаційна зброя – це комплексні технології деструктивного впливу на інформаційні ресурси й інформаційну інфраструктуру, суперника, на індивідуальну і суспільну свідомість, інтервенції в чужий інформаційний простір, за якою завжди слідує інтервенція геополітична і територіальна.

Ключові слова: інформаційна зброя, інформаційна війна, правові засади, гібридна війна, міжнародні конфлікти.

The article clarifies the functioning of information weapons and their legal means in waging information warfare. The means of information warfare are determined using the example of the current Russian-Ukrainian war and other wars. It has been proven that information weapons are complex technologies of destructive influence on information resources and information infrastructure, an opponent, individual and public consciousness, interventions in someone else's information space, which is always followed by geopolitical and territorial intervention.

Keywords: information weapons, information war, legal foundations, hybrid war, international conflicts.

Суб'єкти інформаційних воєн оперують ключовим ресурсом – інформаційною зброєю і застосовують арсенал засобів ведення інформаційного протистояння. Саме існування інформаційної зброї відрізняє інформаційну війну від інших видів конфліктів. Інформаційна зброя – це комплексні технології деструктивного впливу на інформаційні ресурси й інформаційну інфраструктуру, суперника, на індивідуальну і суспільну свідомість, інтервенції в чужий інформаційний простір, за якою завжди слідує інтервенція геополітична і територіальна. Так, Наталія Войтович зазначає, що в сучасній ситуації почастишали приклади того, «коли з метою досягнення політичних цілей засоби масової інформації застосовуються замість збройних сил» [12, С. 70]. Подібне явище спостерігали десятиліттями під час російських інформаційних атак, коли головним інструментом російської влади були засоби масової комунікації. Зрештою, це призвело до анексії Криму і до російсько-української війни.

Мета дослідження з'ясувати функціонування інформаційної зброї і її правових засобів у веденні інформаційної війни. Відповідно до поставленої мети нами визначено таке

завдання – визначити засоби інформаційної війни на прикладі актуальної російсько-української війни й інших воєн.

Теоретичну основу нашого дослідження слали праці І. Валюшко, Н. Войтович, Я. Жаркова, С. Полумієнко, А. Стадника, Г. Фороса.

Вважаємо за доцільне детальніше проаналізувати підходи до визначення інформаційної зброї, позаяк саме вона є диференційною ознакою інформаційної війни. Дослідниця Г. Форос у розвідці «Сучасний стан розвитку інформаційної протидії» пише, що інформаційна зброя – це «засоби інформаційно-технічного характеру, які знищують, перекручують або викрадають інформацію, не зважаючи на систему захисту, обмеження доступу до цієї інформації законних користувачів, а також інформаційно-психологічні засоби, які дезорганізують інформаційні системи шляхом дезінформації, формування помилкових логічних інформаційних концепцій, інтерпретацій та ін., впливаючи таким чином на думку суспільства та на функціонування органів влади» [6, С. 146].

Аналізуючи роль інформаційної зброї в сучасних міжнародних конфліктах, І. Валюшко у статті «Еволюція інформаційних війн: історія і сучасність» зазначає, що «інформаційна зброя дозволяє вигравати війни, не вдаючись до звичайної зброї. Інформаційна зброя співставляється зі зброєю масового знищення, вона не вимагає спеціальних засобів виробництва або складної інфраструктури для використання. Засоби інформаційної війни – це програмне забезпечення, апаратні засоби комп'ютерних вірусів, логічних бомб тощо. Ці активи і методи інформаційної війни поєднують відносно низьку собівартість виробництва та високу ефективність як під час війни, так і в мирний час» [1, С. 132]. Я. Жарков у праці «Інформаційна безпека особистості, суспільства, держави» зазначає, що в американській фаховій класифікації розглядають дев'ять різновидів інформаційної зброї, які доцільно об'єднати в чотири групи: засоби впливу на інформаційну інфраструктуру; засоби розвідки, отримання інформації з інформаційних, телекомунікаційних і подібних систем; засоби впливу на інформацію, яка обробляється в інформаційних системах, наприклад, на програмно-математичне забезпечення цих систем; засоби впливу на суспільну свідомість [3, С. 110].

Ця класифікація є доволі прозорою та чіткою для ідентифікації інформаційної зброї. Галина Стадник також наголошує на таких показниках інформаційної зброї, як: «цілеспрямованість, вибірковість, масштабність впливу, досяжність, швидкість доставки, комплексність впливу на людей, технічні засоби і системи, можливість регулювання (дозування) «потужності» впливу», визначаючи її як зброю масового впливу. Також, за її словами, інформаційній зброї притаманні додаткові особливості: «атакувальний характер, універсальність, скритність, багатоваріантність форм реалізації, радикальність впливу, псевдовибірковість, свобода просторово-часового маневру, економічність, які роблять інформаційну зброю надзвичайно привабливою і небезпечною» [5, С. 114].

Окрім цього, як вказує Яків Жарков, провідні країни мають власні спеціалізовані служби, основною функцією яких є використання інформаційної зброї: наприклад, Агентство національної безпеки (NSA) у США, Штаб-квартира урядового зв'язку (HGC) у Великобританії, Німецька служба інформаційної безпеки (BSI) і Агентство національної безпеки Бундесверу у Німеччині тощо [3, С. 110].

Журналістикознавиця Н. Войтович вказує, цитуючи російського політолога І. Панаріна, на 19 найпоширеніших прийомів інформаційної війни, які багато в чому збігаються із загальною типологією маніпулятивних технологій у ЗМІ та ЗМК:

1. «Приклеювання або навішування ярликів», тобто застосування негативних і образливих художніх засобів, порівнянь, метафоричних назв для найменування людини, організації, ідеї, будь-якого соціального явища. «Ярлики» спонукають до емоційно негативного ставлення й негативних асоціацій, наприклад, у свідомості росіян Львів надійно

засоційований із ідеологічними соціально-культурними концептами-ярликами «фашизм», «нацисти» і «бандерівці».

2. «Покликання на авторитет», тобто апелювання до великих авторитетів (як негативних, так і позитивних у свідомості реципієнтів). Як наголошує Наталія Войтович, після анексії Криму у російських засобах масової інформації почали транслювати повідомлення про підтримку політики Володимира Путіна на українському півострові відомими російськими зірками шоу-бізнесу, які користуються високим рівнем суспільної довіри в Росії.

3. «Підтасування карт» відбувається тоді, коли ЗМІ/ЗМК демонструють вибірково і виключно позитивні або лише негативні факти й докази при замовчуванні протилежних їм ідей чи доказів.

8. «Висміювання» – прийом, який однаково можуть використовувати для дискредитації людини, ідеї, проєкту, організації тощо. Прикладом цього може бути висміювання прихильників українського Майдану у російських ЗМК, де часто озвучували пейоративний журналістський термін «майданути».

9. Поширення чуток є ефективним методом інформаційного протистояння, хоча він має короткотривалий вплив. Наприклад, під час Революції Гідності соціальні мережі рясніли фейками і неперевіреною інформацією, що поширювалася із блискавичною швидкістю.

10. Провокації – відома технологія інформаційної війни, яка «рятуює» ситуацію, коли потрібних реальних інформаційних приводів нема чи не вистачає. Тут доречно пригадати брехливі повідомлення російського телеканалу «24» про побиття майданівцями «беркутівців». А в березні 2014 року в ефірі російського телеканалу «Дощ» Леонід Ярмольник запевняв, що бачив на власні очі повішання місцевими чорношкірого на берегах у Львові лише через його залицяння до львівської дівчини.

11. «Захоплення медіапростору», тобто узурпація його одним ЗМК, як це відбулося під час анексії Криму, коли Росія повністю заблокувала доступ до українських ЗМК.

12. «Ствердження». Поширення тверджень у ролі «незаперечних фактів», які нерідко можуть бути маніпулятивними чи брехливими.

13. «Вимушена пропаганда», тобто застосування імперативів і спонукальних конструкцій. Наприклад, під час виборчої кампанії партії часто користуються гаслам: «Голосуй за» і «Обери».

14. «Громадське несхвалення» – це типовий метод творення ілюзії суспільного осуду (з допомогою маніпулятивних соціологічних даних, підтасування висловлювань «із народу»).

15. «Пряме спростування».

16. «Порушення логічних і часових зв'язків між подіями» дозволяє ефективно змінити суть повідомлення і зробити бажаний маніпулятивний акцент.

17. «Заміна джерела повідомлення». Метод полягає в заміні джерела повідомлення для збільшення або зменшення довіри до повідомлення залежно від рівня суспільної довіри до джерела.

18. «Формування оточення».

19. «Применшення значущості теми», тобто банальне зміщення акцентів із важливого на несуттєве, з негативного на нейтральне чи суперечливе [2, С. 70]. Відзначимо, щоправда, що при класифікації методології інформаційних воєн дослідниця не розмежовує інформаційні «акції, заходи та операції», ані маніпулятивні технології.

Сергій Полумієнко в розвідці «Гібридна війна, її окремі передумови, стратегії та наслідки», здійснивши відповідний аналіз, пропонує власну структуру стратегій у гібридних війнах. Дослідник, зокрема, наголошує на тій обставині, що всі такі стратегії спрямовані на заміщення на арені міжнародних відносин політичними стратегіями. Серед основних сценаріїв, згідно з дослідником, слід назвати такі:

1. Визначення та пропагандування свого вигаданого «історичного походження» й інтересів у країні-жертві (як-от, радянська концепція «колиски трьох братів» і походження зі спільної Київської Русі), публічне підтримання думки про потребу захисту російськомовного населення.

2. Інформаційна «обробка» свого (російського) населення, заміна реальних критеріїв державного успіху і суспільного добробуту уявними політичними цілями (будівництво «світлого майбутнього»), постійна інформаційна підготовка людей до «неминучої» війни чи воєнного конфлікту, переакцентування внутрішніх проблем на зовнішні (нерідко вигадані).

3. Масована пропаганда в інших країнах і регіонах задля створення лояльного оточення й підтримки, зокрема, й шляхом залучення суспільних авторитетів.

4. Контроль ключових підприємств, зокрема, через ринкові механізми.

5. Формування та дислокація військових підрозділів, комплектування військових груп на території максимально близько до кордону з країною-суперником.

6. Формулювання суспільного образу «ворога» й типова радянська стратегія війни з «усім світом», тобто з тими країнами, на які складно чи неможливо безпосередньо вплинути.

7. Нехтування міжнародними угодами й документами чи переінтерпретування їх у вигідному для своїх політичних інтересів світлі.

8. Нехтування інтересами, життям і добробутом населення (зокрема, власного). Публічна й показова «гуманітарна допомога».

9. Створення й підтримка національних, регіональних і міжнародних об'єднань, угруповань, окремих осіб з метою їх використання для переорієнтації суспільства та політиків на власні цілі, знищення всіх сфер життя у їхній країні.

10. Розмивання меж миру і війни, порядку і хаосу, створення єдиної зони ризику, де країна-агресор обов'язково потребує бути «гарантом» миру та спокою. Результатом впровадження такої стратегії є сфера впливу – держава або група буферних держав.

11. Встановлення, використання й позірна підтримка урядів-маріонеток, квазіурядів.

12. Використання для своїх цілей економіки, територій країн-маріонеток, створення мережевої структури таких держав, як центрів дезорганізації нормального життя.

13. Застосування силових ресурсів і військових стратегій (при істотній військовій перевазі) під прикриттям.

14. Руйнація економіки й інфраструктури країни-жертви [4, С. 78].

Як бачимо, дослідники загалом збігаються в поглядах на методи і засоби ведення інформаційної війни Росією проти України й оцінці актуальних подій у цій сфері.

Отже, суб'єкти інформаційних воєн оперують ключовим ресурсом – інформаційною зброєю і застосовують арсенал засобів ведення інформаційного протистояння. Саме існування інформаційної зброї відрізняє інформаційну війну від інших видів конфліктів. Інформаційна зброя, згідно з різними підходами, – це комплексні технології деструктивного впливу на інформаційні ресурси й інформаційну інфраструктуру, суперника, на індивідуальну і суспільну свідомість, інтервенції в чужий інформаційний простір, за якою завжди слідує інтервенція геополітична і територіальна.

1. Валюшко І. Еволюція інформаційних війн: історія і сучасність. *Історико-політичні студії. Сер. Політичні науки* : зб. наук. пр. / М-во освіти і науки України, ДВНЗ «Київ. нац. екон. ун-т ім. Вадима Гетьмана», Ін-т історії укр. сусп-ва ; редкол.: І. Д. Дудко (голова) та ін. Київ : КНЕУ, 2015. № 2. С. 127–134.
2. Войтович Н. О., Кравець Р. К. Сучасна інформаційна війна: Росія проти України. *Обрії друкарства*. 2014. № 1. С. 69–78.
3. Жарков Я., Дзюба М. Т., Замаруєва І. В. Інформаційна безпека особистості, суспільства, держави : підручник. Київ : Видавничо-поліграфічний центр «Київський університет», 2008. 274 с.
4. Полумієнко С. Гібридна війна, її окремі передумови, стратегії та наслідки. *Вісник Національної академії наук України*. 2017. № 8. С. 72–82.
5. Стадник А. Інформаційна війна як комунікативна технологія впливу на масову свідомість та громадську думку. *Грані*. 2016. № 1. С. 111–115.
6. Форос Г. Сучасний стан розвитку інформаційної протидії. *Правова держава*. 2012. № 15. С. 336–340.